PHYSICAL LAYER SECURITY IN THE 5G HETEROGENEOUS WIRELESS SYSTEM WITH IMPERFECT CSI

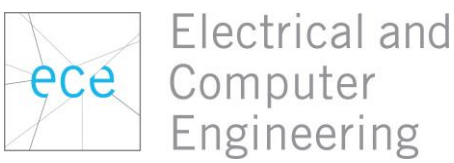
Marc Franch Isart

MSc Thesis

Department of Electrical and Computer Engineering,
Institute for Computing, Information and Cognitive Systems
University of British Columbia

Escola Tècnica Superior d'Enginyeria de Telecomunicació de Barcelona,
Universitat Politècnica de Catalunya

Supervised by:
Prof. Zehua Wang
Prof. Victor C.M. Leung
Prof. Jordi Casademont Serra



VANCOUVER, CANADA. June 2020

Title of the thesis: Physical layer security in the 5G heterogeneous wireless system with imperfect CSI

Author: Marc Franch Isart

Advisors: Zehua Wang, Victor C.M. Leung and Jordi Casademont Serra

Abstract

5G is expected to serve completely heterogeneous scenarios where devices with low or high software and hardware complexity will coexist. This entails a security challenge because low complexity devices such as IoT sensors must still have secrecy in their communications. This project proposes tools to maximize the secrecy rate in a scenario with legitimate users and eavesdroppers considering: i) the limitation that low complexity users have in computational power and ii) the eavesdroppers' unwillingness to provide their channel state information to the base station. The tools have been designed based on the physical layer security field and solve the resource allocation from two different approaches that are suitable in different use cases: i) using convex optimization theory or ii) using classification neural networks. Results show that, while the convex approach provides the best secrecy performance, the learning approach is a good alternative for dynamic scenarios or when wanting to save transmitting power.

UNIVERSITAT POLITÈCNICA DE CATALUNYA BARCELONATECH

THE UNIVERSITY OF BRITISH COLUMBIA

Acknowledgements

Firstly, I want to acknowledge Dr. Victor C.M. Leung for accepting me in his research group and giving me the opportunity to move to Vancouver to conduct research at the University of British Columbia in the Department of Electrical and Computer Engineering. During all these months, he has always been ready to help me whenever I needed it.

I would also like to show my gratitude to Dr. Zehua Wang for co-supervising and helping me during all the project here in Vancouver and for all the inspiring and priceless meetings that we had. It has been really useful to have the opportunity to weekly discuss all the progress made and exchange ideas about the steps done.

Additionally, I would also want to thank all the researchers at the Communications Lab for the useful discussions that we had explaining each other's projects and trying to constructively contribute to them. It has been a pleasure to work with you during all these months here in Vancouver and to share time with you outside the lab. To all the other friends that I made in Vancouver, thank you for making my stay so good and the memorable moments.

Finally, thanks to Dr. Jordi Casademont Serra for co-supervising my thesis from Barcelona and the help offered by him whenever I needed it.

Summary of original work

The following publications have been reported within the research conducted in this Master's Thesis:

M. Franch Isart, Z. Wang and V. C.M. Leung, "Physical layer security in heterogeneous MIMO wireless networks with imperfect CSI: a deep learning approach". *Prepared for INFOCOM 2021.*

Revision history and approval record

Revision	Date	Purpose
0	07/04/2020	Document creation
1	19/06/2020	Document revision

Written by:		Reviewed and approved by:	
Date	03/06/2020	Date	01/07/2020
Name	Marc Franch Isart	Name	Z. Wang and V. C.M. Leung
Position	Project Author	Position	Project Supervisors

Table of contents

List of Figures

List of Tables

1. Introduction

1.1. Motivation

The fifth generation (5G) wireless communication networks are expected to be a completely heterogeneous networking system (*i.e.,* devices of different complexity will be served by the same base station (BS)). This is taken into account in the standardization process of 5G, where three main use scenarios have been defined and designed to satisfy different needs: the enhanced mobile broadband (eMBB), the massive machine type communications (mMTC) and the ultra-reliable low-latency communications (URLLC). To serve the different needs, each of these three use scenarios addresses either low or high complexity devices, but not both at the same time. This is why complex and simple devices will coexist in the 5G scenario.

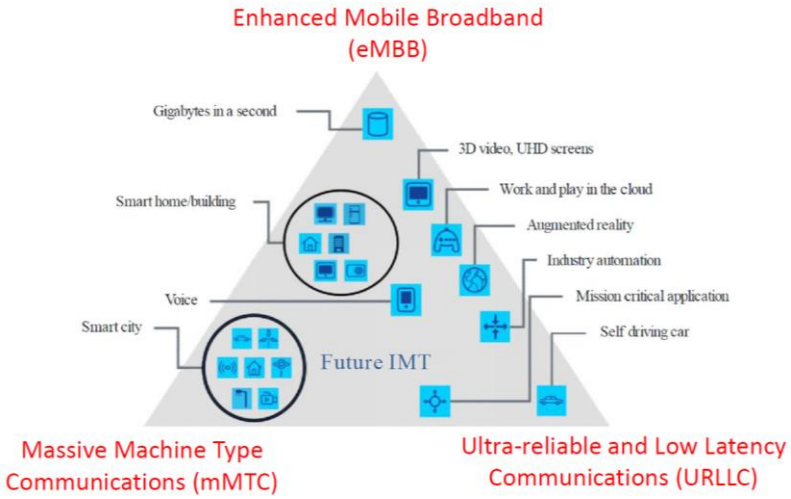


Figure 1 Main scenarios designed for 5G networks. (Source: IMT Vision – "Framework and overall objectives of the future development of IMT for 2020 and beyond")

To achieve the immense capacity promised by the eMBB use scenario, techniques such as massive multiple-input multiple-output (MIMO) [1] have been studied. These techniques are expected to be deployed in the majority of 5G devices because they seek to achieve higher spectral and energy efficiency. The fundamental idea behind the massive MIMO techniques is using a large number of antennas in the device. This leads to the novel concept of *spatial multiplexing*, which consists in having multiple simultaneous transmissions (each of them called a *stream*) exchanging different information. However, this idea of having multiple antennas in the device has the cost of increasing both hardware and software complexity. This is particularly important in one of the use scenarios foreseen in 5G: the mMTC. This use case has been designed for the Internet of Things (IoT) field, which is going to gain importance in both private and public industries. The tendency is already seen in sectors such as smart homes or smart cities. Additionally, the devices that make these sectors possible are basically sensors that have strong requirements for low power consumption, long battery life, and limited computational capabilities.

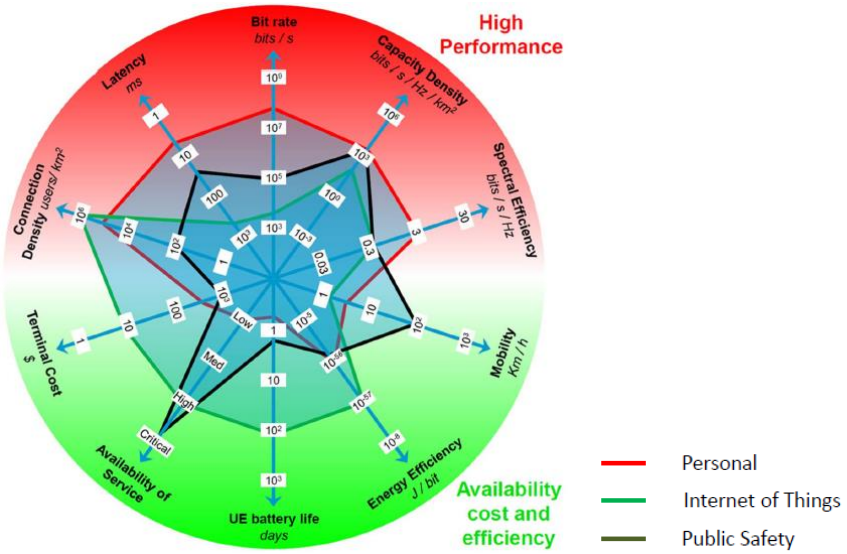


Figure 2 Requirements for the personal and Internet of Things devices. (Source: IMT Vision – "Framework and overall objectives of the future development of IMT for 2020 and beyond")

An essential characteristic of wireless communications is security. Security was first introduced in the second generation (2G) wireless communication systems and the new functionalities foreseen for 5G must not compromise it. Secure communications prevent others from spying, stealing or using other users' information. Up to the current fourth generation (4G), security has been achieved by traditional cryptographic tools which might not be compatible with the IoT devices' computational capabilities. This problem entails a challenge to be solved, where both high and low complexity devices must achieve secrecy in their communications. It should be noticed that, under the IoT framework, many public safety and emergency use cases will appear and will completely rely on secure communications.

A great alternative to the traditional cryptographic tools when dealing with low complexity devices is physical layer security, a field based on information theory [2] that can guarantee secret communications even in low complexity devices. To achieve that, the approach is using tools such as precoding, channel inversion techniques, signal processing or artificial noise injection [3] and [4]. This approach is somehow different to the traditional techniques because it seeks to guarantee security by using the wireless channel's imperfections (*e.g.,* noise or fading) as a source of security [1]. However, the heterogeneity of devices might impact the implementation of physical layer security approaches. The main concept behind this field is the channel state information (CSI), because knowing the channel is the only way of using its imperfections to get secure communications. In this sense, not only the legitimate receiver's CSI has to be considered but also some malicious users (*i.e.,* eavesdroppers) might be present in the network.

Considering the worst case scenario, the multi-antenna eavesdroppers might have very powerful computing capabilities and be even more powerful than the legitimate users. This means that, if traditional cryptography methods were used, eavesdroppers would have an advantage over legitimate users. In addition, these eavesdroppers may not want to reveal their existence (*i.e.,* CSI of the eavesdroppers is not known) and the transmission should not be compromised because of this fact. Additionally, affordable IoT devices with low complexity might not be capable of estimating the channel and providing it as feedback to the BS. This means that the channel has to

be estimated at the BS by using the information in the uplink signals and this differs from traditional smartphone users. In the smartphone users' case, the channel is estimated by the users' device and sent to the BS as feedback.

Considering that in 5G the amount of connected devices is expected to grow exponentially [5], handling and using the information generated by all the users might be tricky. This information does not only include application data but also CSI or other metrics that might be useful for the allocation of resources. Machine learning has led to robust and precise results in a big variety of fields [6] such as medicine, automotive industry, social media or sales. In the wireless communications field, many studies have also used machine learning for modulation and activity recognition [7] and [8], forecasting traffic [9] or detecting anomalies [10]. Therefore, applying deep learning seems a promising approach to extract features and make decisions based on the information provided by users. Additionally, this approach would be robust to the uncertainty or corruption that noise introduces to data [11]. By using learning tools, the latency associated to resource allocation processes could be significantly reduced when comparing it with traditional optimization problems.

1.2. Statement of purpose

Motivated by the possibility explained in the previous subsection, this Master's Thesis considers the heterogeneous wireless system with imperfect CSI and studies the maximization of the secrecy rate for multiple users. It also provides an important novelty in the physical layer field: a deep learning system that leverages the maximization study to perform the resource allocation that achieves secrecy performance. Additionally, in our study we also consider the power efficiency of the resource allocation: the achieved secrecy rate over the transmitting power used by the BS. This is especially important in the 5G framework, where the BS densification process will lead to smaller service areas. Then, the operator of the network might be interested in using low power when transmitting to obtain an advantage in terms of frequency reuse in adjacent cells. Power efficiency will give us a quantification of the existing trade-off between secrecy performance and power used.

To achieve the maximization of the secrecy rate for multiple users, this document proposes a convex optimization-based problem that solves the resource allocation for considered 5G scenarios. These scenarios consider a multi-antenna architecture at the BS, some legitimate users that need to receive confidential information but that might have very low computational capabilities, and some powerful eavesdroppers that might be trying to spy the legitimate users. The maximization study considers possible uncertainty associated to the fact that eavesdroppers might not want to reveal their CSI and also takes into account possible interference requirements that the mobile network operator (MNO) might set for the users.

Regarding the deep learning system, the proposed study uses the so-called classification neural networks to use historical data in order to predict the best resource allocation that leads to secrecy performance. In this way, the study details aspects such as the architecture of the neural networks used, the training set acquisition or the training process.

1.3. Requirements and specifications

The project requirements are:

- It has to propose a mathematical notation that can be used to model any physical layer security scenario.
- The notation has to be used in an optimization problem that solves the resource allocation to provide secrecy performance.
- A convex optimization-based problem has to be proposed, as the project seeks to find the optimal resource allocation to achieve the desired secrecy in communications.
- Constraints derived from low complexity legitimate receivers have to be considered in the study.
- It has to provide an alternative way to compute the resource allocation. This is, although the convex problem will lead to the resource allocation that achieves best secrecy performance, it may not be suitable for dynamic environments where the channel conditions change very fast. Then, an alternative approach needs to be proposed.
- Alternative approaches proposed might show a worse performance than the convex algorithm but have to provide higher performance than a random allocation.
- Power efficiency constraints must be considered towards frequency reuse in the 5G framework with densification of BSs.

The specifications are:

- The study will consider a TDD-based transmission so that the CSI available at the BS can always be used to compute the resource allocation.
- The resource allocation computed will consider downlink transmissions in a multi-antenna BS.
- There will be a limited available transmitting power at the BS. The proposed resource allocation cannot use more than this available power.

1.4. Methods and procedures

This document uses the classical mathematical notation used in a great variety of fields. The specific notation used is the following: $\mathbf{X}$ is a matrix, $\mathbf{x}$ is a vector and x is a scalar. $\mathbf{X}^H$ is the conjugate transpose, $\mathbf{X}^*$ is the conjugate, $\mathrm{Tr}(\mathbf{X})$ is the trace and Rank($\mathbf{X}$) is the rank of matrix $\mathbf{X}$. $\mathcal{CN}(0,\sigma^2)$ is a complex Gaussian distribution with zero-mean and variance σ^2. $\mathbb{C}$ is a complex number, $\mathbb{C}^{m\times n}$ is an $m \times n$ matrix with complex components and $\mathbb{H}^{mn}$ is an Hermitian matrix of size $m \cdot n$. $|\cdot|$ is the absolute value operator, $\|\cdot\|$ is the Euclidean norm, $\mathfrak{Re}$ is the real part operator and $\mathfrak{Im}$ is the imaginary part operator. $\mathbf{X} \succeq \mathbf{0}$ indicates that $\mathbf{X}$ is a positive semidefinite matrix, $\mathbf{I}_N$ is an identity matrix of size $N \times N$ and $\mathbf{0}_N$ is a $N \times 1$ vector with all elements equal to 0.

1.5. Work plan and Gantt diagram

The detailed work plan and the Gantt diagram of the project can be reviewed in the appendix of the document.

1.6. Description of the deviations from the initial plan and incidences

No big deviations occurred during the development of the project, but during the last stage the coronavirus pandemic impacted our work by forcing us to work remotely for some time. This led to some technical difficulties when trying to access to servers to perform long simulations, as some of them had time limits when using them. This had the impact of making the process of obtaining results slower.

1.7. Methodology

After the motivation, statement of purpose, requirements and specifications have been explained, the methodology followed in this thesis is explained and mapped to the sections of the document. Section 2 reviews the state of the art and contains the necessary background regarding physical layer security and using deep learning at the physical layer. It also reviews some mathematical tools used in the project to analyze optimization problems. After that, Section 3 presents the convex optimization approach that solves the resource allocation towards secrecy performance. It details the steps followed from the initial non-convex optimization problem to the final algorithm which makes use of an iterative algorithm that solves a series of convex problems. The constraints derived from practical considerations are explained and formulated after presenting the mathematical formulation used.

Section 4 presents the learning system designed in our work. There we detail all the architecture, inputs and outputs of the proposed neural networks as well as all the considerations involved in the acquisition of the training set and training of the networks. The section also explains the existing links between the convex algorithm proposed in Section 3 with the actual learning system. Finally, Section 5 shows the results obtained, where we detail representative figures from our study, compare the performance of three algorithms (*i.e.,* the convex algorithm, the learning system and a random allocation) and discuss the suitability of each of them. Section 5 also focuses on the proposed learning system and analyzes the correlation of performance and the training set size. Additional results study the impact of low velocity users in our study. Then, Section 6 contains the conclusions of the project.

After reading all the sections in the document and understanding both the proposed mathematical optimization and learning system, the reader will be able to clearly identify the differences between the proposed tools and the suitability of using each of them depending on the use case. The summary of the proposed tools is depicted in Figure 3.

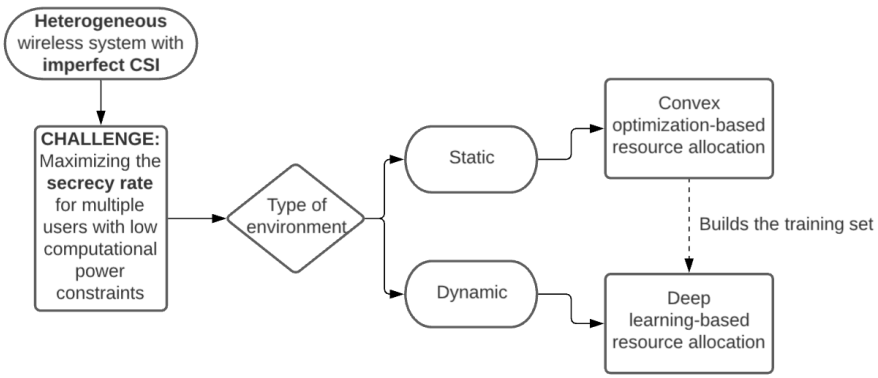


Figure 3 Block diagram containing the tools proposed in our study

1.8. Competences

To elaborate the work contained in the project, some research on various topics has been done. This report contains all the information to be able to understand all the steps followed and ideas proposed but the reader should keep in mind that the competences needed include concepts from convex optimization, MATLAB's library *CVX*, beamforming and multi-antenna techniques, physical layer security metrics, knowledge of classification neural networks and some general mathematical tools.

2. State of the art

This section will give basic understanding on the main tools used in the project: convex optimization, the physical layer security field and classification neural networks. After this is done, a review of the literature is included to let the reader know relevant research conducted on the subject.

2.1. Convex optimization

This section aims to give a short and very simplified overview of the convex optimization field. Convex optimization is a field within mathematical optimization problems that has the advantage that very efficient solving techniques can be used to solve this kind of problems and find an optimal solution. However, in order that a given optimization problem is convex there is the need that both the cost function and the constraints follow very strict conditions. As seen during the work done in Section 3 of this report, even if the initial given problem is not convex there are many ways to relax the problem and end up obtaining a convex optimization problem.

The basic structure of a convex optimization problem is the following:

$$\begin{aligned} \min_{\mathbf{x}} \quad & f_0(\mathbf{x}) \\ \text{s.t.} \quad & f_i(\mathbf{x}) \leq b_i, \qquad i = 1, ..., m \\ & h_i(\mathbf{x}) = 0, \qquad i = 1, ..., p \end{aligned}$$

As seen, we have either a maximization or minimization problem with a cost or objective function that depends on the optimization variable **x** and whose result is a scalar. In the same problem we might have more than one optimization variables that can be scalars, vectors or matrices. Regarding the constraints, we have two types: the inequality constraints and the equality constraints. Then, in the case of a maximization problem we want to find the value of **x** that leads to having the largest possible value of the cost function but that satisfies all the listed consraints. In the case of a minimization problem we want the opposite, finding the **x** that satisfies all the constraints and that leads to the minimum possible value of the cost function.

Regarding the strict conditions that the cost function and the constraints need to follow to form a convex problem, we have the following:

- All the functions $f_0, f_1, \ldots, f_m$ must be convex functions, a mathematical property that refers to the functions that satisfy $f_i(\alpha\mathbf{x} + \beta\mathbf{y}) \leq \alpha f_i(\mathbf{x}) + \beta f_i(\mathbf{y})$ for $\mathbf{x}, \mathbf{y} \in \Re^n, \alpha, \beta \in \Re, \alpha + \beta = 1, \alpha \geq 0$ and $\beta \geq 0$.
- All the equality constraint functions must be affine functions, meaning that $h_i(x) = \alpha_i x - \beta_i$.

On the other hand, the main advantage of using convex optimization problems is the existing efficient methods to solve them. All the existing methods use the fact that convex functions only have one local minimum (*i.e.,* the global minimum).

It is very helpful that the reader has these very basic ideas clear and to keep them in mind while reading the thesis report. To help understanding the steps followed in Section 3, and as a clear summary of this subsection, we propose Figure 4.

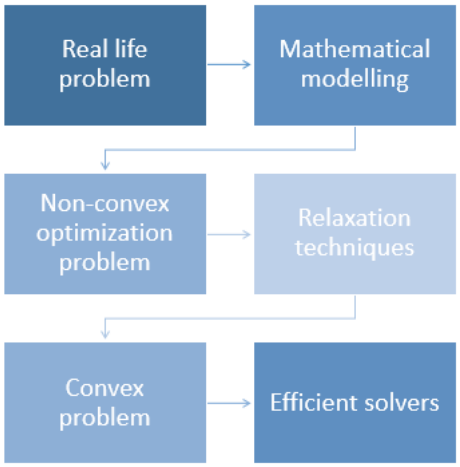


Figure 4 Steps from real problems to convex optimization-based solutions.

2.2. Physical layer security

One of the most used and simple tools to depict the problem of security in wireless communication system is using the so-called fading wiretap channel [1] depicted in Figure 5. As seen, there is one transmitter Alice that wants to send information to a legitimate receiver Bob but the wireless channel introduces fading and noise to the transmitted signal. However, there is a malicious user called Eve who wants to secretly spy Bob and listens to the transmitted information. Due to the wireless link between Alice and Eve, the information that Eve receives is also affected by a different fading and noise when compared to what Bob receives. Then, the aim of security techniques is that the mutual information between what Alice transmits and what Eve receives has to tend to zero when the message is sufficiently long. This is that, even Eve is listening to the communication between Alice and Bob, Eve should not be able to extract information from it.

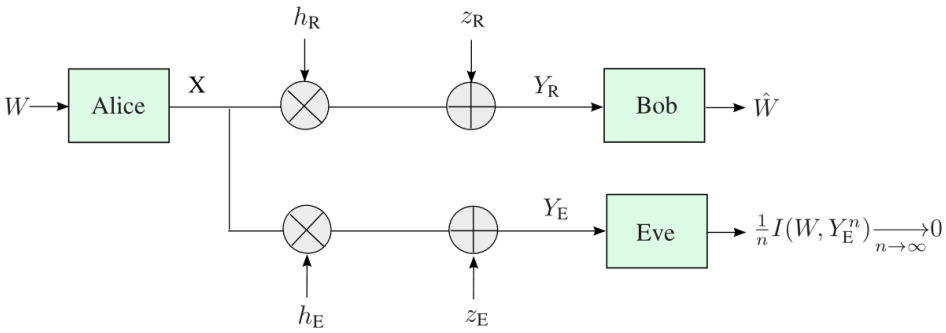


Figure 5 Fading wiretap channel

A field that is becoming popular to implement security in the communication is physical layer security. The main reason behind the appearance of physical layer security is clearly depicted in Section 1.1, being especially important with the mMTC scenario that will be present in 5G. This is due to the fact that physical layer security achieves secure communications by exploiting features from the lowest layer of the communications systems: the physical layer. Until now, the most common approach to achieve secure communications has been by working in the high layers to implement more computationally complex cryptographic techniques. However, physical layer aims to leverage the properties that are naturally found in the wireless channel such as the fluctuations of the channel, the randomness or noise. This means that even very low complexity

devices can achieve secrecy in their communications without the need of performing complex computations with the signals that they receive. Some examples of the techniques used in the physical layer field will be referenced in Section 2.4, but to give an idea they range from a wide variety of approaches: using artificial noise injection to deteriorate the eavesdroppers receiving conditions, using cooperative methods to let relays in the network implement these noise injection techniques, using relays that know accurately the CSI to amplify and forward the information to the legitimate users, exploiting the noisy channel to generate keys between the legitimate users, transmit antenna selection schemes to leverage the available CSI or using phase rotation techniques based on the CSI.

In this work, to achieve secrecy performance through physical layer security, we focus on the multi-antenna structure of the BS. In this way, we are going to understand the antennas as an antenna array and we are going to feed each of them with a different gain and phase. By modifying these parameters, the interference between the fields of each radiated field and the actual channel status will build a certain radiation pattern that will make possible having secrecy in our communications. This is, the eavesdroppers are going to have unfavorable receiving conditions while the legitimate receivers will have the opposite.

Additionally, as it is going to be explained in Section 3.1, we are going to assume that CSI is available at the BS. Then, we should first provide a basic overview of how the channel estimation is performed when using orthogonal frequency-division multiplexing (OFDM) technology, the scheme used in 5G networks. Starting with the typical smartphone case, the channel estimation is done at the UE. This is, the BS will send reference signals to the users so that they are used in the UE for channel estimation. The way to do it is specified in 3GPP-LTE specifications, so that all the BSs will implement it in the same way. Then, the specifications say that the BSs can transmit three types of reference signals: cell-specific reference signals, UE-specific reference signals and multicast-broadcast single frequency network reference signals. To keep it simple, let's explain the case of the cell-specific reference signals as it is the most used case. First of all, the resource allocation in OFDM is defined by a set of resource elements. These resource elements are defined by subcarriers in the frequency domain and symbols in the time domain, which is a mapping of the signals that the BS transmits. Then, LTE specifications specify that the cell-specific reference signals must be placed only in specific positions of the time-frequency grid, and these positions will be determined by the Physical Layer Cell Identity used in the communication, a parameter that the UE determines after decoding the primary and secondary synchronization signals. Then, the possible allocations of the cell-specific reference signals for the different Physical Layer Cell Identity values are depicted in Figure 6. These allocations cycle once every six Physical Layer Cell Identities, meaning that the structure is repeated every six identities.

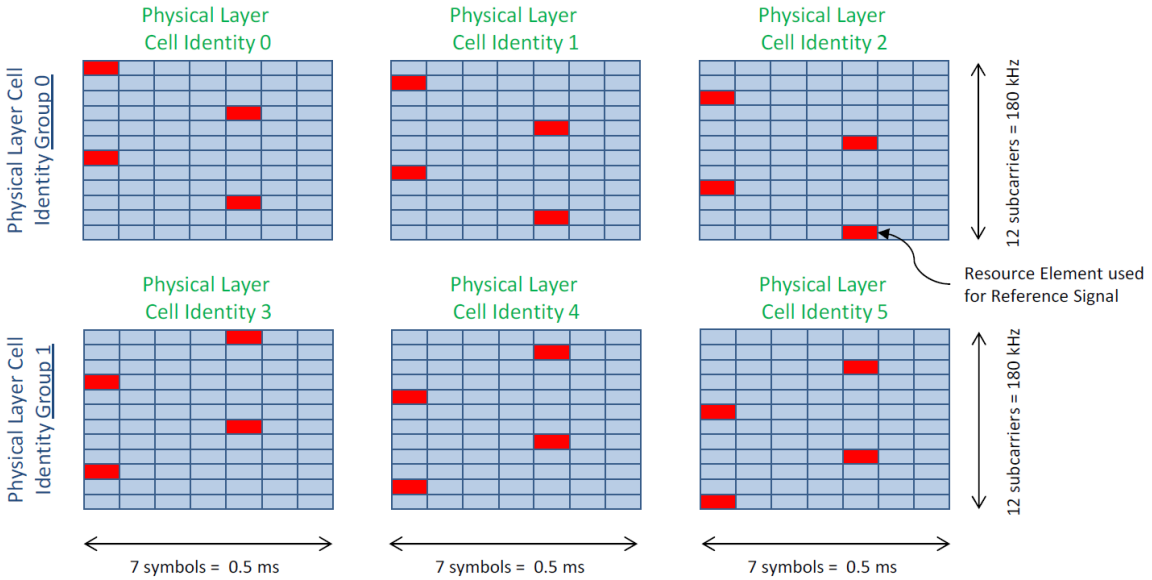


Figure 6 Mapping of the cell-specific reference signals as a function of the Physical Layer Cell Identity for the short-prefix case.

As said, after the UE has decoded the primary and secondary synchronization signals, it will know the Physical Layer Cell Identity and this will mean that the UE also knows both the resource elements allocated to the cell-specific reference signals and the sequence used to generate the reference signal. Then, the UE will extract the reference signals from the received signals and the channel transfer function can be estimated. Some common methods that the UEs use to estimate the channel from these known received reference signals are based on the least square and linear minimum mean square error criteria. Finally, the CSI extracted by using this process is sent as feedback to the BS for the resource allocation.

However, for the low complexity devices obtaining the CSI follows a different process. Having low complexity means that the least square or linear minimum mean square error cannot be performed at the device. This makes that, in this case, devices transmit uplink pilot sequences that will be used by the BS to determine the CSI. It is important that these sequences are mutually orthogonal from one low complexity device to the other. Then, the BS would be able to use these received pilot sequences to extract the CSI for future resource allocation provided that there is a TDD channel reciprocity assumption as detailed in Section 3.

2.3. Classification neural networks

The main idea behind machine learning and the reason why we introduced it in our work is that by using this tool we can construct algorithms that can learn from big sets of data. Then, this learning will allow us to obtain accurate predictions when we face similar data in future situations. We can define different types of machine learning problems based on the information that we have available when performing this training. The type that we are going to use in our work is supervised learning, which consists on predicting a target from a set of available inputs. In supervised learning we perform the training using what we call a training set, composed of a set of labeled examples from which the system is going to learn. This means that based on these examples the system will predict in future situations which has to be the output based on the inputs that we feed into it.

In the field of supervised learning we can still categorize the problems depending on the output that we want to obtain (*e.g.,* classification or regression), but in our work we are only going to work with classification techniques. This is, from a set of inputs that we are going to feed into the network, we expect to obtain a category or *class* as output. Then, in our case, we are going to have some inputs defining our wireless communication network and we are going to assign a class which will correspond to a beamforming strategy that meets our needs. The approach followed in this work to perform the classification process is using neural networks. The basic component of a neural network is a neuron, which is modeled by the perceptron model and detailed in Figure 7.

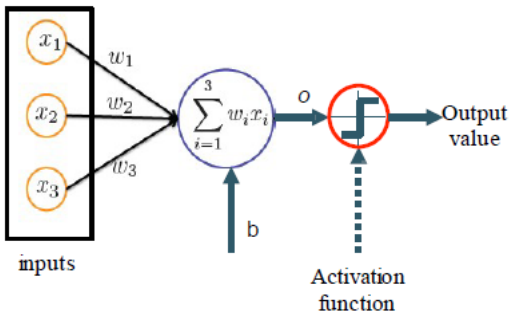


Figure 7 Neuron with three inputs.

This is, we have some inputs to what we call the neuron and we associate a weight to each input. Then, the operation of the neuron is to compute the linear combination of the inputs and weights plus a given bias. Once we have obtained the result of that, we can apply a nonlinear activation function to obtain the output value, meaning that this activation function will define the output given the set of inputs. Based on the output value we can then classify the input data, but in the case of just using one neuron we will only be capable of classifying linearly separated problems.

To classify more complex problems that are not linearly separated problems, we need to use networks with more capacity than just a single neuron. Then, here appears the idea of multi-layer neural networks depicted in Figure 8. This idea consists on stacking neurons to combine them until we achieve the capacity that we need. The basic structure of a multi-layer neural network consists of three blocks: the input layer, the hidden layers and the output layer. The input layer is simple and contains just the input data fed into the network. However, the hidden layers are where all the neurons of the networks are included and where we combine them. We can have many hidden layers and each of them is going to be composed by a given number of neurons that operate as explained for the basic neuron case. The output of one neuron will be used as input of the neurons in the following hidden layers, meaning that each of the neurons in that hidden layer will operate in the same way as the single neuron case. Regarding the output layer there are many types, but for the multiclass classification case it will consist of multiple output nodes (each output corresponding to one class). To map the output of the last hidden layer with the classes represented by the output layer, what is used is the softmax activation function. This function converts the output of the last hidden layer into a predicted probability for each class. Then, the output of the multiclass classification network will be the class with highest predicted probability.

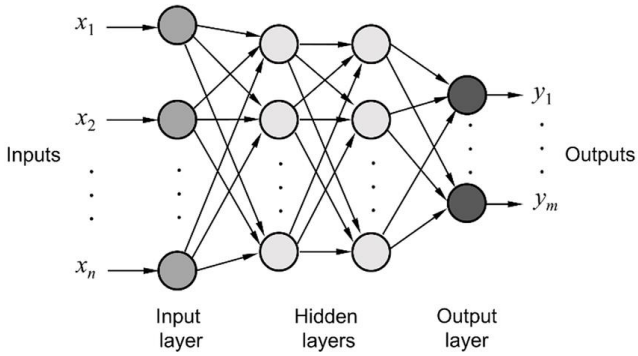


Figure 8 Multi-layer neural network.

Finally, it is worth saying that when designing neural networks with multiple hidden layers there are lots of aspects to consider. The architecture of the neural network is defined by multiple *hyperparameters*, which are variables that give shape to the neural network. Some of the most basic hyperparameters considered, and the ones that have been set in our work, are the number of neurons (*i.e.,* nodes) in each hidden layer, the number of hidden layers, the type of activation function in each node or the weight initialization strategy. Besides these, more advanced hyperparameters have also been designed in our work to obtain good performance in our classification. These hyperparameters include the learning rate, the regularization constant to prevent from overfitting (*i.e.,* happens when the system is memorizing the input rather than learning), the dropout factor or the number of epochs (*i.e.,* iteration over all examples).

2.4. Related work

The adoption of deep learning in the wireless networks field has started to be studied in literature applied to the different open system intercommunication (OSI) layers (*e.g.,* the physical layer, the data link layer, the network layer or upper layers) [12]. Focusing on the physical layer, the use cases vary and include studies such as anti-jamming communications [13] or modulation classification techniques [14]. Following this trend, data-driven algorithms have been proposed in [15] to exploit big volumes of data. The data is used to address the radio resource allocation in radio access networks (RANs) and avoid relying on the traditional and computationally complex mathematical optimization-based algorithms. In [15], features are extracted from the different key performance indicators (KPIs) and are used in the deep learning-based resource allocation.

Numerous studies, as the one in [7], prove that by using deep learning-based algorithms we can achieve competitive performance levels compared to the traditional techniques. However, for the best of our knowledge, there has not been much work done applying deep learning to the physical layer security framework. Some recent publications such as [16] consider the MIMO channel with the presence of eavesdroppers and propose a learning-based algorithm for the transmit antenna selection process based on the CSI of the different users to achieve secrecy performance. Other works such as [17] continue the common trend followed by the majority of works done applying deep learning to the physical layer security. This trend uses relays to achieve secrecy performance by computing the modulated signals at the output of the relays using a deep neural network.

On the other hand, the physical layer security problem has been widely studied using traditional tools. A common trend is considering uncertainty associated to the CSI available at the

transmitter [1] and the tools used to achieve secrecy vary from study to study (*e.g.,* using precoding techniques [18] or using noise injection approaches [19]). After analyzing the common aspects in the traditional works, we realized that there was the need to work on deep learning approaches in physical layer security. There are very few works done on deep learning applied to CSI, an information which is crucial for the physical layer security. The works done either address the problem of reconstructing CSI in noisy environments where the data may be inaccurate [11] or seek to reduce the feedback required in CSI transmission [20]-[22].

Recent works [23], [24] considering physical layer security assume the MIMO framework that will be common in the upcoming 5G wireless system. To this end, traditional physical layer security expressions have been adapted to the interference MIMO system [25], [26].

3. Convex optimization-based resource allocation

This section of the document details our proposed convex optimization-based resource allocation to optimize the global secrecy rate in a scenario with eavesdroppers and legitimate receivers. This solution is going to be used later in the document as the base of the learning-based resource allocation that we propose.

3.1. System model

In this subsection, we detail the system model assuming heterogeneous conditions. Based on Wyner's work [27] in the definition of the wiretap channel, let us consider that *K* legitimate users with different hardware and software complexities are receiving data from the BS under a time division duplex-based (TDD-based) transmission. Additionally, in the considered transmission the channel remains constant for a coherence time interval enabling channel reciprocity. Under this general assumption that the legitimate users can have different complexity levels, we consider that there might be some single-antenna ones while at the same time others might use the massive MIMO technology envisioned in 5G scenarios.

As mentioned in Section 1.1, the single-antenna devices might be sensors belonging to the IoT and therefore have interest in using physical layer security. The advantage of doing so is having an alternative to the traditional cryptographic tools to avoid the computational cost involved. Regarding the BS, and continuing with the 5G scenario assumption, a massive MIMO architecture is considered with N_{bs} antennas. Then, to assume the worst possible scenario, there may be more than one powerful eavesdroppers in the scenario equipped with a massive MIMO architecture and N_e antennas trying to obtain the information directed towards the legitimate users. As a general assumption, these eavesdroppers are considered to be passive and trying to obtain information from the users. The corresponding system model is shown in Figure 9.

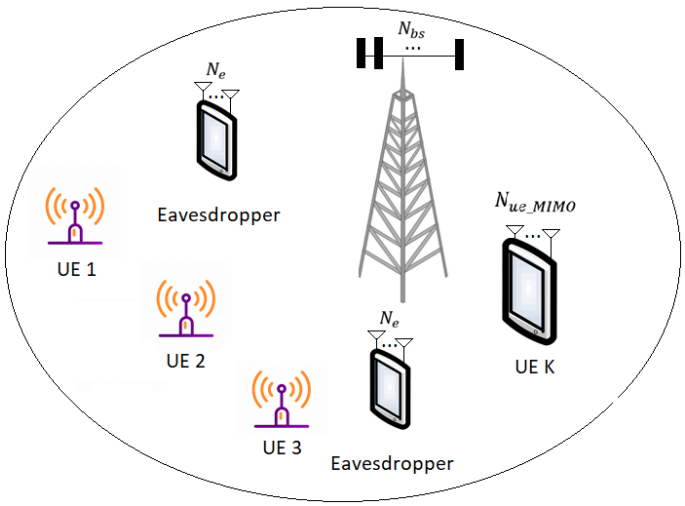


Figure 9: Heterogeneous system model considered.

To approach the problem, we consider that some CSI is available at the BS but might be subject to some uncertainty. As a first approach to the problem, we consider that the legitimate users' CSI is always known accurately by the BS and therefore we assume perfect knowledge of this CSI. Note that there might be uncertainty in the estimation of this CSI since the information

might get corrupted due to the noisy environment but works such as [11] address this problem and can achieve accurate CSI in this kind of scenarios. On the other hand, the eavesdroppers do not want to reveal their existence and the BS can only have a statistical knowledge of their CSI (*i.e.,* imperfect CSI) based on historical data of past scenarios. This knowledge can be used under stationary and static environment assumptions with a low number of obstacles moving around. Having this statistical knowledge means that, unlike the legitimate receivers' CSI case, we are going to assume uncertainty associated to the eavesdroppers' CSI. This uncertainty is going to be modelled to have a bound for the circle in a higher dimension of space where the real CSI value is going to be [28]. This concept of statistical CSI knowledge is considered in [1], where the authors state that at least statistical CSI at the transmitter is needed to achieve some level of information theoretic security.

As we are considering different complexity levels in the user equipment (UE) due to the modelled heterogeneous scenario, the way of obtaining the legitimate receivers' CSI is different depending on the type of UE. In the case of high complexity UE (*i.e.,* non-IoT devices), the CSI is sent as feedback from the UEs to the BS after estimating it by using downlink signals. However, for the low complexity devices (*i.e.,* IoT environment) the approach to obtain the CSI is by using uplink pilot signals [29]. In both cases, the CSI is assumed to be an independent and identically distributed (i.i.d.) complex Gaussian random variable $\mathcal{CN}(0,1)$ because the channel model considered for all the links is the independent Rayleigh fading. Then, the massive MIMO architecture is considered so that the antennas are always separated more than half a wavelength.

Regarding the physical resources used, the multi-antenna devices are assumed to use the classical OFDM technology where different subcarriers are linked to a different CSI (technology used in 4G and 5G networks). However, the IoT devices or single-antenna devices are going to use either NB-IoT or LTE-M technology and this will determine the number of subcarriers that they use in either uplink or downlink.

3.2. Problem formulation

3.2.1. Channel model

For the sake of narrowing down to a specific case, in this problem formulation we are modelling the UEs as single-antenna devices, which is basically taking the single-antenna case as a special case of the MIMO case. Note that the work presented in this report can be applied to the multiple-antenna UE case by just modelling the UE's channel model by a matrix and not a vector. Additionally, in the system model we considered channel reciprocity and this means that we could eventually assume that the same CSI can be used for the downlink and uplink cases. This report focuses on the downlink case as a starting point, where the BS transmits both to complex and simple UE in the presence of powerful eavesdroppers. As stated in the previous section, the channel distribution for all the links is going to be an i.i.d. complex Gaussian random variable $\mathcal{CN}(0,1)$. Under these assumptions, we are going to model the following two channels: i) the link between the massive MIMO BS and the single-antenna UE and ii) the link between the massive

MIMO BS and the massive MIMO eavesdroppers. Starting with the first case, let us consider the channel for UE *k*:

$$\mathbf{h}_k = \begin{bmatrix} h_{k,1} \\ h_{k,2} \\ \cdots \\ h_{k,N_{bs}} \end{bmatrix}, \qquad (1)$$

where the first subscript number corresponds to the user *k=1,…,K* and the second subscript corresponds to the antenna number in the BS with *i=1,…,*N_{bs}.

The second case has to consider the MIMO architecture at the eavesdroppers:

$$\mathbf{G}_e = \begin{bmatrix} g_{e_{1,1}} & \cdots & g_{e_{1,N_e}} \\ g_{e_{2,1}} & \cdots & g_{e_{2,N_e}} \\ \cdots & g_{e_{i,l}} & \cdots \\ g_{e_{N_{bs},1}} & \cdots & g_{e_{N_{bs},N_e}} \end{bmatrix}, \qquad (2)$$

where the first subscript number corresponds to the antenna number in the BS with *i=1,…,*N_{bs} and the second subscript corresponds to the antenna number in eavesdropper *e* with *l=1,…,* N_e.

From the second case, it is interesting to introduce a new channel definition. This is the case of the channel between the antennas at the BS and a specific antenna of the eavesdropper (*i.e.,* antenna *m*). To this use, let us define the following:

$$\mathbf{g}_{e,m} = \begin{bmatrix} g_{e_1} \\ g_{e_2} \\ \cdots \\ g_{e_{N_{bs}}} \end{bmatrix}, \qquad (3)$$

where the subscript number on the right-hand side corresponds to the BS's antenna number *i=1,…,*N_{bs}.

3.2.2. Received signals

The signals received at each node can be expressed using the previous channel expressions. As we are modelling the downlink, starting with the received signal at UE *k* sent by the BS:

$$y_k = \mathbf{h}_k^H \mathbf{w}_k s_k + \sum_{i \neq k} \mathbf{h}_k^H \mathbf{w}_i s_i + n_k, \qquad (4)$$

where $y_k \in \mathbb{C}$ is the received signal at UE *k*, $\mathbf{h}_k \in \mathbb{C}^{N_{bs} \times 1}$ corresponds to the channel vector from each antenna in the BS to the receiving antenna in UE *k*, $\mathbf{w}_k \in \mathbb{C}^{N_{bs} \times 1}$ is the beamforming vector at the BS for UE *k*, s_k is the complex and scalar data symbol for UE *k* and $n_k \in \mathbb{C}$ is the noise term associated with user *k* that follows the statistical distribution $\mathcal{CN}(0, \sigma_k^2)$. Notice that in the previous expression there is also a term associated with the interfering signals for all the values of $i \neq k$.

Next, we need to model the received signals at the multi-antenna eavesdroppers which are trying to spy user's *k* information. Let's imagine that we create a set containing the eavesdroppers spying user *k*, then the signal sent by the BS to any eavesdropper in this set can be expressed as:

$$\mathbf{y}_{e,k} = \mathbf{G}_{e,k}^H \mathbf{w}_k s_k + \sum_{i \neq k} \mathbf{G}_{e,k}^H \mathbf{w}_i s_i + \mathbf{n}_{e,k}, \qquad (5)$$

where $\mathbf{y}_{e,k} \in \mathbb{C}^{N_e \times 1}$ is the received signal, $\mathbf{G}_{e,k} \in \mathbb{C}^{N_{bs} \times N_e}$ is the matrix defined in the channels definition part for the eavesdroppers and $\mathbf{n}_{e,k} \in \mathbb{C}^{N_e \times 1}$ follows a $\mathcal{CN}(0, \sigma_e^2)$ distribution and is the noise term associated with any eavesdropper $\mathbf{e}$ of the set spying *k*.

3.2.3. Signal-to-interference-plus-noise ratios

Considering the previous expressions for the received signal at each node and aiming to give an expression for the bit rate, there is the need to propose the following signal-to-interference-plus-noise ratio (SINR) in each case. Starting with the SINR at UE *k*:

$$\gamma_k = \frac{\left|\mathbf{h}_k^H \mathbf{w}_k\right|^2}{\left|\sum_{i \neq k} \mathbf{h}_k^H \mathbf{w}_i\right|^2 + \sigma_k^2}. \qquad (6)$$

While, for the eavesdroppers we have a different situation. As seen in the previous subsection, we see that there is a different signal received in each antenna of the eavesdroppers (due to the MIMO architecture of the eavesdroppers). To specify the SINR at the eavesdroppers, we need to assume the operation of the eavesdropper. In this kind of situations where the receiver is equipped with a MIMO architecture, there are many approaches available to determine the SINR. Some of them make use of what is called coherent combining, a signal processing-based approach where the receiver makes additional computations to coherently combine the signals of each of the antennas to achieve a more favorable value of SINR. Examples of these techniques are the equal-gain combining [30] and the so-called maximum ratio combining [31]. Other techniques are much simpler and avoid extra processing at the receiver. One example is the selection combining technique, where the MIMO receiver just selects the antenna (*i.e.,* branch) with largest instantaneous SINR. In our work, we assume that the eavesdropper wants to decode as much information as possible and therefore any of these techniques where there is an enhancement of the SINR could be considered. For the sake of simplicity and to avoid assuming that the eavesdropper perfectly knows the channel between itself and the BS, our model is going to consider the case of the selection combining technique. In this case, the SINR at the antenna with largest instantaneous SINR will be:

$$\gamma_{e,max} = \frac{\left|\mathbf{g}_{e,max}^H \mathbf{w}_k\right|^2}{\left|\sum_{i \neq k} \mathbf{g}_{e,max}^H \mathbf{w}_i\right|^2 + \sigma_e^2}, \qquad (7)$$

where $\mathbf{g}_{e,max}^H$ refers to the row vector defined in the previous subsection for the antenna with highest instantaneous SINR of the eavesdropper. From now on, we are going to treat the eavesdropper as a single-antenna device by focusing on this best antenna. Therefore, we can use notations such as γ_e to refer to $\gamma_{e,max}$ or $\overline{\mathbf{g}}_e$ to refer to $\mathbf{g}_{e,max}$.

3.2.4. Data rates

The expressions for the bit rate in each case can be computed by using the SINRs defined in the previous subsection. Starting with UE *k*:

$$R_k = B \cdot \log_2(1 + \gamma_k) = B \cdot \log_2\left(1 + \frac{\left|\mathbf{h}_k^H \mathbf{w}_k\right|^2}{\left|\sum_{i \neq k} \mathbf{h}_k^H \mathbf{w}_i\right|^2 + \sigma_k^2}\right). \qquad (8)$$

Now, for an eavesdropper trying to spy user *k*:

$$R_{e,k} = B \cdot \log_2(1 + \gamma_{e,k}) = B \cdot \log_2(1 + \frac{\left|\overline{\mathbf{g}}_e^H \mathbf{w}_k\right|^2}{\left|\sum_{i \neq k} \overline{\mathbf{g}}_e^H \mathbf{w}_i\right|^2 + \sigma_e^2}), \quad (9)$$

where $\overline{\mathbf{g}}_{e,k}$ refers to the channel between all the antennas at the BS and the antenna with maximum SINR of an eavesdropper that is trying to spy user *k*.

Furthermore, one of the metrics for physical layer security is the secrecy rate [1], which is defined by:

$$R_s = \max(R_{legitimate} - R_{eavesdropper}, 0). \quad (10)$$

In this way, and considering the expressions (8)-(10), the secrecy data rate can be defined for our system model:

$$R_s = \max(R_k - R_{e,k}, 0) = \max(B \cdot \log_2(1 + \frac{\left|\mathbf{h}_k^H \mathbf{w}_k\right|^2}{\left|\sum_{i \neq k} \mathbf{h}_k^H \mathbf{w}_i\right|^2 + \sigma_k^2}) - B \cdot \log_2(1 + \frac{\left|\overline{\mathbf{g}}_e^H \mathbf{w}_k\right|^2}{\left|\sum_{i \neq k} \overline{\mathbf{g}}_e^H \mathbf{w}_i\right|^2 + \sigma_e^2}), 0). \quad (11)$$

3.2.5. Optimization problem

Regarding the optimization problem, there are two possible approaches to consider in our model. First, we could try to maximize the secrecy data rate of the users considering a limitation in the available amount of power at the BS and the imperfect CSI knowledge associated with the eavesdroppers. In this way, we would need to find the best resource allocation that leads to good reception conditions for the legitimate users and bad conditions for the eavesdroppers. However, another optimization problem could be trying to minimize the allocated power considering a secrecy data rate that has to be ensured with a given outage probability. After analyzing the two approaches, we have decided to choose the first approach due to the following reasons:

- Considering the project's security framework, it is more suitable to maximize the secrecy data rate.
- It would be difficult to justify the assumption in the value of secrecy data rate that has to be guaranteed with a given outage probability if we selected the power minimization approach.
- In situations where the channel state is not good enough, certain values of secrecy data rate could not be guaranteed even when all the transmit power was used. Instead, it seems more reasonable to maximize the secrecy rate adding a transmit power constraint to the problem.

Once the problem of maximizing the secrecy data rate has been selected, the next step is to model the uncertainty associated with the eavesdroppers' CSI. As assumed in the system model,

the powerful eavesdroppers present in the scenario are not willing to transmit their CSI to the BS but the BS is going to have an imperfect CSI knowledge (*i.e.,* only a statistical knowledge) obtained from the available historical data. For this uncertainty, the model used in [28] is adopted in our study. Then, we model the actual channel between the BS and any eavesdropper as:

$$\overline{\mathbf{g}}_e = \widehat{\mathbf{g}}_e + \Delta\mathbf{g}_e, \quad \forall e \tag{12}$$

$$\Omega_e \triangleq \left\{\Delta\mathbf{g}_e^H \Delta\mathbf{g}_e \leq \varepsilon_e^2\right\}, \quad \forall e \tag{13}$$

where $\overline{\mathbf{g}}_e$ is the instantaneous channel vector for the eavesdropper's antenna with highest uncertainty, $\hat{\mathbf{g}}_e$ is the statistical knowledge of the eavesdropper's CSI (for the same antenna) that the BS has and $\Delta\mathbf{g}_e$ is the CSI uncertainty considered for the antenna. The statistical knowledge of the eavesdropper's CSI that the BS has for the antenna with highest uncertainty is modelled as $\hat{\mathbf{g}}_e \in \mathbb{C}^{N_{bs}\times 1}$ and is clearly not a random variable. As in [28], Ω_e is the uncertainty region and defines a continuous space that contains all the possible values for the channel uncertainty. Additionally, ε_e is a constant that defines the radius of the uncertainty region (*i.e.,* the maximum value of the norm of the vector associated to the eavesdropper's CSI). Note that in this formulation we make the definitions for the antenna with highest value of uncertainty among all the antennas in the eavesdropper. However, we can only find a bound for the uncertainty of all the antennas of the eavesdropper and we cannot know the uncertainty associated to each specific antenna. This means that we can just know the radius of the uncertainty region as a global for all the antennas in the eavesdropper's MIMO architecture.

Regarding the statistical distribution of the term $\Delta\mathbf{g}_e$, we can obtain it by using the definition of the uncertainty region Ω_e and by continuing the trend of modelling the uncertainty as a zero-mean Gaussian CSI error [32],[33]. For the trivial case of two antennas at the BS, and following the definition of the uncertainty region:

$$\begin{bmatrix}\Delta g_{e,1}^* & \Delta g_{e,2}^*\end{bmatrix}\begin{bmatrix}\Delta g_{e,1} \\ \Delta g_{e,2}\end{bmatrix} \leq \varepsilon_e^2, \quad \forall e \tag{14}$$

Considering the zero-mean Gaussian CSI error we have that the term on the left of (14) follows a second order Chi Square distribution (*i.e.,* a Rayleigh distribution). If we assume a symmetric uncertainty both for each antenna and for the real and imaginary part, we have that $|\Delta g_{e,1}|^2 \leq \frac{\varepsilon_e^2}{2}$ and $|\Delta g_{e,2}|^2 \leq \frac{\varepsilon_e^2}{2}$ for $\forall e$. This means that for both antennas $l = 1,2$ and $\forall e$ we have $|\Re\mathrm{e}(\Delta g_{e,l})| \leq \sqrt{\frac{\varepsilon_e^2}{4}}$ and $|\Im\mathrm{m}(\Delta g_{e,l})| \leq \sqrt{\frac{\varepsilon_e^2}{4}}$. From the properties of any Gaussian distribution, following the 68-95-99.7 rule we know that the 99.7% of the distribution is contained between the interval $[\mu - 3\sigma, \mu + 3\sigma]$. Knowing that we are working with a complex Gaussian distribution for the zero-mean Gaussian CSI error, we can model $\Delta g_{e,1}$ and $\Delta g_{e,2}$ as $\Delta g_{e,l} \sim \mathcal{CN}(0, \frac{\varepsilon_e^2}{18})$.

After this modelling, the optimal beamforming at the BS that maximizes the secrecy data rate can be found as:

$$\begin{aligned} \max_{\mathbf{W},\boldsymbol{\varphi}} \quad & \sum_k \max(R_k - R_{e,k}, 0) \\ \text{s.t.} \quad & \sum_k \|\mathbf{w}_k\|^2 \leq p_{bs} \\ & \varphi_{e,k} \geq \max_{\Delta\mathbf{g}_{e,k}\in\Omega_e} \gamma_{e,k} \quad \forall e,k \end{aligned} \tag{15}$$

Note that when going from (11) to (15), as the eavesdroppers' SINRs depend on the CSI uncertainties, we treat these SINRs as optimization variables and include them as constraints of the optimization problem. As we are interested in having low values for these SINRs in the cost function, the constraints have been designed in the worst case scenario so that the optimization variable is equal or greater than the values in the uncertainty region. By proposing this optimization problem we are computing the beamforming that needs to be implemented at the BS to maximize the global secrecy rate (*i.e.,* considering all the legitimate users and eavesdroppers). However, the problem in (15) is not convex. Even if the *max* operator was removed from the cost function, the problem would still not be convex and remain as follows:

$$\begin{aligned} \max_{\mathbf{W},\boldsymbol{\varphi}} \quad & \sum_k (\log_2(1 + \frac{\left|\mathbf{h}_k^H \mathbf{w}_k\right|^2}{\left|\sum_{i\neq k} \mathbf{h}_k^H \mathbf{w}_i\right|^2 + \sigma_k^2}) \\ & \quad - \log_2(1+\varphi_{e,k})) \\ \text{s.t.} \quad & \sum_k \|\mathbf{w}_k\|^2 \leq p_{bs} \\ & \varphi_{e,k} \geq \max_{\Delta\mathbf{g}_{e,k}\in\Omega_e} \gamma_{e,k} \quad \forall k \end{aligned} \tag{16}$$

To obtain a convex problem from this non-convex formulation, some relaxation techniques are proposed in this report. First, following the strategy in [28], we propose an interference decoupling to achieve a more tractable expression for the cost function but with the cost of adding new constraints to the problem. However, in our problem we need to distinguish between the interference perceived by the legitimate users and the interference perceived by the eavesdroppers. Thus, we propose two interference bounds which are going to be considered as predefined, known (*i.e.,* not optimization variables) and a maximum level of interference that the network operator allows the users (*i.e.,* legitimate users and eavesdroppers) to experience. Notice that, by introducing these predefined variables, the amount of interference guaranteed can be easily controlled just by modifying the values. Following this approach, the optimization problem remains as follows:

$$\begin{aligned} \max_{\mathbf{W},\boldsymbol{\varphi}} \quad & \sum_k (\log_2(1 + \frac{\mathrm{Tr}\left(\mathbf{h}_k \mathbf{h}_k^H \mathbf{w}_k \mathbf{w}_k^H\right)}{I_{ue} + \sigma_k^2}) - \log_2(1+\varphi_{e,k})) \\ \text{s.t.} \quad & \sum_k \|\mathbf{w}_k\|^2 \leq p_{bs}, \\ & \varphi_{e,k} \geq \max_{\Delta\mathbf{g}_{e,k}\in\Omega_e} \frac{\mathrm{Tr}\left(\overline{\mathbf{g}}_e \overline{\mathbf{g}}_e^H \mathbf{w}_k \mathbf{w}_k^H\right)}{I_e + \sigma_e^2} \quad \forall k, \\ & I_e \geq \max_{\Delta\mathbf{g}_{e,k}\in\Omega_e} \sum_{i\neq k} \mathrm{Tr}\left(\overline{\mathbf{g}}_e \overline{\mathbf{g}}_e^H \mathbf{w}_i \mathbf{w}_i^H\right), \\ & I_{ue} \geq \sum_{i\neq k} \mathrm{Tr}\left(\mathbf{h}_k \mathbf{h}_k^H \mathbf{w}_i \mathbf{w}_i^H\right). \end{aligned} \tag{17}$$

As seen in (17), we have introduced additional constraints to the problem. Notice that the number of new constraints depends on the number of legitimate users and eavesdroppers, as the interference bound is applied to every user and eavesdropper. Regarding the legitimate users, the constraint introduced controls the interference upper bound (*i.e.,* I_{ue}), making sure that even in the worst case scenario they never experience this level of interference. Note that in this formulation we do not assume a different bound for each of the *K* different legitimate users as we assume the worst case considering them all as a global. In the eavesdroppers' case, the interference bound I_e is a lower bound and refers to the best case scenario while considering all the possible values contained in their CSI uncertainty region.

After applying the interference decoupling, the cost function does not have optimization variables in the denominator anymore. However, the third constraint of the problem (corresponding to the eavesdroppers' interference bound) and the second constraint involve infinitely many inequality constraints due to the mentioned continuity of the space defining the CSI uncertainty region. This problem can be solved by transforming the constraints into Linear Matrix Inequality (LMI) constraints using the S-Procedure [34], a very common approach widely used in literature [28] and [35]. As explained in [34], the S-Procedure is based on the following lemma:

Lemma 1 (S-Procedure [34]): Let $\mathbf{A}_1, \mathbf{A}_2 \in \mathbb{H}^{MN}$, $\mathbf{d}_1, \mathbf{d}_2 \in \mathbb{C}^{MN\times 1}$ and $y_1, y_2 \in \mathbb{R}$. Considering the following two functions of vector $\mathbf{x} \in \mathbb{C}^{MN\times 1}$:

$$\begin{aligned} f_1(\mathbf{x}) &= \mathbf{x}^H \mathbf{A}_1 \mathbf{x} + 2\Re\mathfrak{e}\{\mathbf{d}_1^H \mathbf{x}\} + y_1, \\ f_2(\mathbf{x}) &= \mathbf{x}^H \mathbf{A}_2 \mathbf{x} + 2\Re\mathfrak{e}\{\mathbf{d}_2^H \mathbf{x}\} + y_2, \end{aligned} \tag{18}$$

The implication $f_1(\mathbf{x}) \leq 0 \Rightarrow f_2(\mathbf{x}) \leq 0$ holds if and only if a $\theta \geq 0$ exists such that:

$$\theta \begin{bmatrix} \mathbf{A}_1 & \mathbf{d}_1 \\ \mathbf{d}_1^H & y_1 \end{bmatrix} - \begin{bmatrix} \mathbf{A}_2 & \mathbf{d}_2 \\ \mathbf{d}_2^H & y_2 \end{bmatrix} \succeq \mathbf{0}, \tag{19}$$

as long as there exists a $\tilde{\mathbf{x}}$ that satisfies $f_1(\tilde{\mathbf{x}}) < 0$.

Applying the previous lemma to the eavesdropper's SINR constraint we have:

$$\begin{aligned} &\Delta\mathbf{g}_{e,k}^H \mathbf{I}_{N_{bs}} \Delta\mathbf{g}_{e,k} + 2\Re\mathfrak{e}\{\mathbf{0}_{N_{bs}}^H \Delta\mathbf{g}_{e,k}\} - \epsilon_e^2 \leq 0 \\ &\Rightarrow \Delta\mathbf{g}_{e,k}^H (\mathbf{w}_k \mathbf{w}_k^H) \Delta\mathbf{g}_{e,k} + 2\Re\mathfrak{e}\{(\mathbf{w}_k \mathbf{w}_k^H \widehat{\mathbf{g}}_{e,k})^H \Delta\mathbf{g}_{e,k}\} \\ &\qquad + \widehat{\mathbf{g}}_{e,k}^H (\mathbf{w}_k \mathbf{w}_k^H) \widehat{\mathbf{g}}_{e,k} - \phi_{e,k}(I_e + \sigma_e^2) \leq 0, \end{aligned} \tag{20}$$

if and only if $\theta_{e,k} \geq 0$ such that the following LMI holds:

$$\overline{\mathbf{S}}_{e,k,1}(\varphi_{e,k}, \vartheta_{e,k}) - \mathbf{Q}_{e,k}^H \mathbf{w}_k \mathbf{w}_k^H \mathbf{Q}_{e,k} \succeq \mathbf{0}, \tag{21}$$

where $\overline{\mathbf{S}}_{e,k,1}(\varphi_{e,k}, \vartheta_{e,k})$ is computed as follows:

$$\overline{\mathbf{S}}_{e,k,1} = \begin{bmatrix} \vartheta_{e,k} \mathbf{I}_{N_{bs}} & \mathbf{0}_{N_{bs}} \\ \mathbf{0}_{N_{bs}}^H & \varphi_{e,k}(I_e + \sigma_e^2) - \vartheta_{e,k}\epsilon_e^2 \end{bmatrix} \tag{22}$$

and $\mathbf{Q}_{e,k}$:

$$\mathbf{Q}_{e,k} = \begin{bmatrix} \mathbf{I}_{N_{bs}} & \widehat{\mathbf{g}}_{e,k} \end{bmatrix} \tag{23}$$

This has been obtained by using the fact that $\mathbf{0}_{N_{bs}} \in \Omega_e$ such that $f_1(\mathbf{0}_{N_{bs}}) = -\epsilon_e^2 < 0$.

Now, applying the Lemma to the eavesdropper's interference constraint:

$$\begin{aligned}
&\Delta\mathbf{g}_{e,k}^H\mathbf{I}_{N_{bs}}\Delta\mathbf{g}_{e,k}+2\Re\mathfrak{e}\{\mathbf{0}_{N_{bs}}^H\Delta\mathbf{g}_{e,k}\}-\epsilon_e^2\leq 0\\
&\Rightarrow\Delta\mathbf{g}_{e,k}^H(\sum_{i\neq k}\mathbf{w}_i\mathbf{w}_i^H)\Delta\mathbf{g}_{e,k}+2\Re\mathfrak{e}\left\{((\sum_{i\neq k}\mathbf{w}_i\mathbf{w}_i^H)\widehat{\mathbf{g}}_{e,k})^H\Delta\mathbf{g}_{e,k}\right\}\\
&\quad+\widehat{\mathbf{g}}_{e,k}^H(\sum_{i\neq k}\mathbf{w}_i\mathbf{w}_i^H)\widehat{\mathbf{g}}_{e,k}-I_e\leq 0,
\end{aligned}\tag{24}$$

if and only if $\varrho_{e,k}\geq 0$ such that the following LMI holds:

$$\overline{\mathbf{S}}_{e,k,2}(\varrho_{e,k})-\mathbf{Q}_{e,k}^H(\sum_{i\neq k}\mathbf{w}_i\mathbf{w}_i^H)\mathbf{Q}_{e,k}\succeq\mathbf{0},\tag{25}$$

where $\overline{\mathbf{S}}_{e,k,2}(\varrho_{e,k})$ is computed as follows:

$$\overline{\mathbf{S}}_{e,k,2}=\begin{bmatrix}\varrho_{e,k}\mathbf{I}_{N_{bs}} & \mathbf{0}_{N_{bs}}\\ \mathbf{0}_{N_{bs}}^H & I_e-\varrho_{e,k}\epsilon^2\end{bmatrix}\tag{26}$$

and the same $\mathbf{Q}_{e,k}$ term as in (23).

Using the previous expressions, the optimization problem is the following:

$$\begin{aligned}
\max_{\mathbf{W},\boldsymbol{\varphi},\boldsymbol{\vartheta},\boldsymbol{\varrho}}\quad & \sum_k(\log_2(1+\frac{\mathrm{Tr}(\mathbf{h}_k\mathbf{h}_k^H\mathbf{w}_k\mathbf{w}_k^H)}{I_{ue}+\sigma_k^2}) && \text{(27a)}\\
& \quad-\log_2(1+\varphi_{e,k}))\\
\text{s.t.}\quad & \sum_k\|\mathbf{w}_k\|^2\leq p_{bs}, && \text{(27b)}\\
& \overline{\mathbf{S}}_{e,k,1}(\varphi_{e,k},\vartheta_{e,k})-\mathbf{Q}_{e,k}^H\mathbf{w}_k\mathbf{w}_k^H\mathbf{Q}_{e,k}\succeq\mathbf{0}, && \text{(27c)}\\
& \overline{\mathbf{S}}_{e,k,2}(\varrho_{e,k})-\mathbf{Q}_{e,k}^H(\sum_{i\neq k}\mathbf{w}_i\mathbf{w}_i^H)\mathbf{Q}_{e,k}\succeq\mathbf{0}, && \text{(27d)}\\
& I_{ue}\geq\sum_{i\neq k}\mathrm{Tr}(\mathbf{h}_k\mathbf{h}_k^H\mathbf{w}_i\mathbf{w}_i^H), && \text{(27e)}\\
& \vartheta_{e,k}\geq 0,\varrho_{e,k}\geq 0, && \text{(27f)}
\end{aligned}$$

where constraints (27c) and (27d) have been obtained after applying the S-Procedure and indicate that the left side of the constraint are positive semidefinite matrices.

However, we still have not achieved a convex problem because of the $\varphi_{e,k}$ term in the cost function. To this end, we propose an iterative algorithm that makes use of the Taylor series approximation to solve the convex optimization problem, inspired by what the authors in [36] did. This step is possible because, going back to the second constraint in (17), we see that $\varphi_{e,k}$ (*i.e.,* an optimization variable) is setting an upper bound for the SINR of the eavesdroppers considering the extreme value for the uncertainty region and the interference at the eavesdroppers but the aim of our work is that it takes a low value. Consequently, as Section 5.2 will show, this will lead to having values close to zero for the SINR and our assumption makes sense. After applying the Taylor series approximation, the convex optimization problem is the following:

$$
\begin{aligned}
\max_{\mathbf{W},\boldsymbol{\varphi},\boldsymbol{\vartheta},\boldsymbol{\varrho}} \quad & \sum_k \log_2(1+\frac{\mathrm{Tr}(\mathbf{h}_k\mathbf{h}_k^H\mathbf{w}_k\mathbf{w}_k^H)}{I_{ue}+\sigma_k^2}) - \log_2(1+\widetilde{\varphi}_{e,k}) \\
& -\frac{1}{\ln(2)}\frac{1}{1+\widetilde{\varphi}_{e,k}}\varphi_{e,k} + \frac{1}{\ln(2)}\frac{1}{1+\widetilde{\varphi}_{e,k}}\widetilde{\varphi}_{e,k} \\
\text{s.t.} \quad & \sum_k \|\mathbf{w}_k\|^2 \le p_{bs} \\
& \overline{\mathbf{S}}_{e,k,1}(\varphi_{e,k},\vartheta_{e,k}) - \mathbf{Q}_{e,k}^H\mathbf{w}_k\mathbf{w}_k^H\mathbf{Q}_{e,k} \succeq \mathbf{0} \\
& \overline{\mathbf{S}}_{e,k,2}(\varrho_{e,k}) - \mathbf{Q}_{e,k}^H(\sum_{i\neq k}\mathbf{w}_i\mathbf{w}_i^H)\mathbf{Q}_{e,k} \succeq \mathbf{0} \\
& I_{ue} \ge \sum_{i\neq k}\mathrm{Tr}(\mathbf{h}_k\mathbf{h}_k^H\mathbf{w}_i\mathbf{w}_i^H) \\
& \vartheta_{e,k} \ge 0, \varrho_{e,k} \ge 0
\end{aligned} \tag{28}
$$

Then, the iterative algorithm will solve the convex problem multiple times until we achieve the desired performance: departing from an initial value, the algorithm will update in each iteration the value $\widetilde{\varphi}_{e,k}$ with the optimal value of $\varphi_{e,k}$ found as a solution to the convex problem. To initialize the value in the first iteration we propose $\widetilde{\varphi}_{e,k} = 0$.

Each iteration of the iterative algorithm will solve the problem in (28). This can be efficiently done with convex optimization solvers like MATLAB's toolbox CVX [37] by making use of the semidefinite programming mode (SDP). However, when using it, the quadratic forms of the optimization variables must be removed. These quadratic terms only appear when multiplying beamforming vectors and, to avoid this multiplication, we propose using a new variable $\mathbf{W}_k$:

$$\mathbf{W}_k = \mathbf{w}_k\mathbf{w}_k^H, \tag{29}$$

where for $N_{bs} = 2$:

$$\mathbf{W}_k = \begin{bmatrix} w_1w_1^* & w_1w_2^* \\ w_2w_1^* & w_2w_2^* \end{bmatrix}, \tag{30}$$

and this must be a rank-one matrix so that the problem is equivalent to the initial one. Once we find a solution for $\mathbf{W}_k$, we will be able to easily recover the information about the phase of each beamforming component by obtaining the singular value decomposition (SVD) of the matrix. Therefore, we have:

$$
\begin{aligned}
\max_{\mathbf{W},\boldsymbol{\varphi},\boldsymbol{\vartheta},\boldsymbol{\varrho}} \quad & \sum_k (\log_2(1+\frac{\mathrm{Tr}(\mathbf{h}_k\mathbf{h}_k^H\mathbf{w}_k\mathbf{w}_k^H)}{I_{ue}+\sigma_k^2}) - \log_2(1+\widetilde{\varphi}_{e,k}) \\
& - \frac{1}{\ln(2)}\frac{1}{1+\widetilde{\varphi}_{e,k}}\varphi_{e,k} + \frac{1}{\ln(2)}\frac{1}{1+\widetilde{\varphi}_{e,k}}\widetilde{\varphi}_{e,k}) \\
\text{s.t.} \quad & \sum_k \|\mathbf{w}_k\|^2 \le p_{bs} \\
& \overline{\mathbf{S}}_{e,k,1}(\varphi_{e,k},\vartheta_{e,k}) - \mathbf{Q}_{e,k}^H\mathbf{w}_k\mathbf{w}_k^H\mathbf{Q}_{e,k} \succeq \mathbf{0} \\
& \overline{\mathbf{S}}_{e,k,2}(\varrho_{e,k}) - \mathbf{Q}_{e,k}^H(\sum_{i\neq k}\mathbf{w}_i\mathbf{w}_i^H)\mathbf{Q}_{e,k} \succeq \mathbf{0} \\
& I_{ue} \ge \sum_{i\neq k}\mathrm{Tr}(\mathbf{h}_k\mathbf{h}_k^H\mathbf{w}_i\mathbf{w}_i^H) \\
& \vartheta_{e,k} \ge 0, \varrho_{e,k} \ge 0, \\
& \mathrm{Rank}(\mathbf{W}_k) \le 1, \\
& \mathbf{W}_k \succeq 0.
\end{aligned} \tag{31}
$$

At first, adding an additional constraint stating that $\mathbf{W}_k$ has to be a rank-one matrix might seem a problem. However, we can remove this constraint from (31) to relax the problem. We can perform this relaxation because of the following theorem:

Theorem 1: Denoting $\varphi_{e,k}^*$ and $\mathbf{W}_k^*$ as the optimal solutions of $\varphi_{e,k}$ and $\mathbf{W}_k$ respectively in the following problem:

$$
\begin{aligned}
\max_{\mathbf{W},\boldsymbol{\varphi},\boldsymbol{\vartheta},\boldsymbol{\varrho}} \quad & \sum_k (\log_2(1+\frac{\mathrm{Tr}(\mathbf{h}_k\mathbf{h}_k^H\mathbf{w}_k\mathbf{w}_k^H)}{I_{ue}+\sigma_k^2}) - \log_2(1+\widetilde{\varphi}_{e,k}) \\
& - \frac{1}{\ln(2)}\frac{1}{1+\widetilde{\varphi}_{e,k}}\varphi_{e,k} + \frac{1}{\ln(2)}\frac{1}{1+\widetilde{\varphi}_{e,k}}\widetilde{\varphi}_{e,k}) \\
\text{s.t.} \quad & \sum_k \|\mathbf{w}_k\|^2 \le p_{bs} \\
& \overline{\mathbf{S}}_{e,k,1}(\varphi_{e,k},\vartheta_{e,k}) - \mathbf{Q}_{e,k}^H\mathbf{w}_k\mathbf{w}_k^H\mathbf{Q}_{e,k} \succeq \mathbf{0} \\
& \overline{\mathbf{S}}_{e,k,2}(\varrho_{e,k}) - \mathbf{Q}_{e,k}^H(\sum_{i\neq k}\mathbf{w}_i\mathbf{w}_i^H)\mathbf{Q}_{e,k} \succeq \mathbf{0} \\
& I_{ue} \ge \sum_{i\neq k}\mathrm{Tr}(\mathbf{h}_k\mathbf{h}_k^H\mathbf{w}_i\mathbf{w}_i^H) \\
& \vartheta_{e,k} \ge 0, \varrho_{e,k} \ge 0, \\
& \mathbf{W}_k \succeq 0,
\end{aligned} \tag{32}
$$

there will always be the possibility of obtaining the optimal solution $[\varphi_{e,k}^*, \overline{\mathbf{W}}_k^*]$ for (31) having $\mathrm{Rank}(\overline{\mathbf{W}}_k^*) \le 1, \forall\, k$. To proof it, we have developed the following: let us consider the original problem in (32). To show this proof, we define a new optimization variable η and define the following equivalent optimization problem by using $\mathbf{H}_k = \mathbf{h}_k\mathbf{h}_k^H$:

$$\max_{\mathbf{W},\boldsymbol{\eta},\boldsymbol{\varphi}_e,\boldsymbol{\vartheta},\boldsymbol{\varrho}} \quad \sum_k (\log_2(1+\eta_k) - c\,\varphi_{e,k} + d) \tag{33a}$$

$$\text{s.t.} \quad \sum_k \mathrm{Tr}(\mathbf{W}_k) \leq p_{bs}, \tag{33b}$$

$$\eta_k \leq \frac{\mathrm{Tr}(\mathbf{H}_k \mathbf{W}_k)}{I_{ue} + \sigma_k^2}, \ \forall k, \tag{33c}$$

$$\overline{\mathbf{S}}_{e,k,1}(\varphi_{e,k}, \vartheta_{e,k}) - \mathbf{Q}_{e,k}^H \mathbf{W}_k \mathbf{Q}_{e,k} \succeq \mathbf{0}, \ \forall k, \tag{33d}$$

$$\overline{\mathbf{S}}_{e,k,2}(\varrho_{e,k}) - \sum_{i \neq k} \mathbf{Q}_{e,k}^H \mathbf{W}_i \mathbf{Q}_{e,k} \succeq \mathbf{0}, \ \forall k, \tag{33e}$$

$$I_{ue} \geq \sum_{i \neq k} \mathrm{Tr}(\mathbf{H}_k \mathbf{W}_i), \ \forall k, \tag{33f}$$

$$\mathbf{W}_k \succeq \mathbf{0}, \ \forall k, \tag{33g}$$

$$\vartheta_{e,k} \geq 0, \varrho_{e,k} \geq 0, \ \forall k. \tag{33h}$$

Then, from the problem in (33), we extract the optimal solution for η and $\varphi_{e,k}$ (*i.e.,* $\eta_k^\star$ and $\varphi_{e,k}^\star$) but we suppose that the solution found for $\mathbf{W}_k^*$ is not rank-one. To find the optimal rank-one solution we can formulate the following problem:

$$\min_{\mathbf{W},\boldsymbol{\vartheta},\boldsymbol{\varrho}} \quad \sum_k \mathrm{Tr}(\mathbf{W}_k) \tag{34a}$$

$$\text{s.t.} \quad \sum_k \mathrm{Tr}(\mathbf{W}_k) \leq p_{bs}, \tag{34b}$$

$$\eta_k^\star \leq \frac{\mathrm{Tr}(\mathbf{H}_k \mathbf{W}_k)}{I_{ue} + \sigma_k^2}, \ \forall k, \tag{34c}$$

$$\overline{\mathbf{S}}_{e,k,1}(\varphi_{e,k}^\star, \vartheta_{e,k}) - \mathbf{Q}_{e,k}^H \mathbf{W}_k \mathbf{Q}_{e,k} \succeq \mathbf{0}, \ \forall k, \tag{34d}$$

$$\overline{\mathbf{S}}_{e,k,2}(\varrho_{e,k}) - \sum_{i \neq k} \mathbf{Q}_{e,k}^H \mathbf{W}_i \mathbf{Q}_{e,k} \succeq \mathbf{0}, \ \forall k, \tag{34e}$$

$$I_{ue} \geq \sum_{i \neq k} \mathrm{Tr}(\mathbf{H}_k \mathbf{W}_i), \ \forall k, \tag{34f}$$

$$\mathbf{W}_k \succeq \mathbf{0}, \ \forall k, \tag{34g}$$

$$\vartheta_{e,k} \geq 0, \varrho_{e,k} \geq 0, \ \forall k. \tag{34h}$$

The particular thing about this problem is that, when it is solved, the solutions for $\overline{\mathbf{W}}_k^*$ and $\eta_k^\star$ satisfy all the constraints in problem (33) and result in having the same cost function value in (33) as solutions $\eta_k^\star$ and $\mathbf{W}_k^*$ found when directly solving (33). For this proof we are going to use the mathematical theory of Karush-Kuhn-Tucker (KKT) conditions. Let's consider two of the KKT conditions of the problem in (34). First, for the stationary KKT condition we have $\nabla_{\mathbf{W}_k} \mathcal{L} = 0$. Then, for the complementary slackness KKT condition we have $\mathbf{V}_k \cdot \mathbf{W}_k = \mathbf{0}$. But to use these two conditions we first need to find the Lagrangian of the problem:

$$
\begin{aligned}
&\mathcal{L}(\mathbf{W},\boldsymbol{\theta},\boldsymbol{\rho},\boldsymbol{\Lambda}) = \\
&\sum_k \mathrm{Tr}\left(\mathbf{W}_k\right) + \lambda_1[\sum_k \mathrm{Tr}\left(\mathbf{W}_k\right) - p_{bs}] \\
&+ \sum_k \lambda_{3,k}[\sum_{i\neq k} \mathrm{Tr}\left(\mathbf{H}_k\mathbf{W}_i - I_{ue}\right)] \\
&+ \sum_k \lambda_{2,k}[\eta_k^\star - \frac{\mathrm{Tr}\left(\mathbf{H}_k\mathbf{W}_k\right)}{I_{ue}+\sigma_k^2}] \\
&+ \sum_k \mathrm{Tr}\left[\mathbf{L}_{1,k}(\mathbf{Q}_{e,k}^H\mathbf{W}_k\mathbf{Q}_{e,k} - \overline{\mathbf{S}}_{e,k,1}(\varphi_{e,k}^\star,\vartheta_{e,k}))\right] \\
&+ \sum_k \mathrm{Tr}\left[\mathbf{L}_{2,k}((\sum_{i\neq k}\mathbf{Q}_{e,k}^H\mathbf{W}_i\mathbf{Q}_{e,k}) - \overline{\mathbf{S}}_{e,k,2}(\rho_{e,k}))\right] \\
&- \mathrm{Tr}\left(\mathbf{V}_k\mathbf{W}_k\right) - \sum_k \zeta_{1,k}\theta_{e,k} - \sum_k \zeta_{2,k}\rho_{e,k},
\end{aligned}
\tag{35}
$$

where we defined $\boldsymbol{\Lambda} = (\lambda_1, \boldsymbol{\lambda}_2, \boldsymbol{\lambda}_3, \mathbf{L}_1, \mathbf{L}_2, \mathbf{V}, \boldsymbol{\zeta}_1, \boldsymbol{\zeta}_2)$ containing the dual variables. From here we are interested in extracting the $\mathbf{W}_k$ term as a common factor in the expression of the Lagrangian. This means that we need to rearrange some terms and find the way to replace the $\mathbf{W}_i$ terms with an expression containing $\mathbf{W}_k$ terms but that has to be equivalent. After some computations, we reach the following result:

$$
\begin{aligned}
&\mathcal{L}(\mathbf{W},\boldsymbol{\theta},\boldsymbol{\rho},\boldsymbol{\Lambda}) = \\
&\sum_k \mathrm{Tr}\left(\mathbf{W}_k\right) + \sum_k \mathrm{Tr}\left(\mathbf{W}_k\lambda_1\mathbf{I}_{N_{bs}}\right) - \lambda_1 p_{bs} \\
&+ \sum_k \mathrm{Tr}\left(\mathbf{W}_k\sum_{i\neq k}\lambda_{3,i}\mathbf{H}_i\right) - \sum_k \lambda_{3,k} I_{ue} \\
&+ \sum_k \lambda_{2,k}\eta_k^\star - \sum_k \mathrm{Tr}\left(\mathbf{W}_k\frac{\lambda_{2,k}\mathbf{H}_k}{I_{ue}+\sigma_k^2}\right) \\
&+ \sum_k \mathrm{Tr}\left(\mathbf{W}_k\mathbf{Q}_{e,k}\mathbf{L}_{1,k}\mathbf{Q}_{e,k}^H\right) - \sum_k \mathrm{Tr}\left(\mathbf{L}_{1,k}\overline{\mathbf{S}}_{e,k,1}(\varphi_{e,k}^\star,\vartheta_{e,k})\right) \\
&+ \sum_k \mathrm{Tr}\left(\mathbf{W}_k\sum_{i\neq k}\mathbf{Q}_{e,i}\mathbf{L}_{2,i}\mathbf{Q}_{e,i}^H\right) - \sum_k \mathrm{Tr}\left(\mathbf{L}_{2,k}\overline{\mathbf{S}}_{e,k,2}(\rho_{e,k})\right) \\
&- \mathrm{Tr}\left(\mathbf{V}_k\mathbf{W}_k\right) - \sum_k \zeta_{1,k}\theta_{e,k} - \sum_k \zeta_{2,k}\rho_{e,k}.
\end{aligned}
\tag{36}
$$

It is simple from (36) to extract the common factor $\mathbf{W}_k$:

$$
\begin{aligned}
&\mathcal{L}(\mathbf{W},\boldsymbol{\theta},\boldsymbol{\rho},\boldsymbol{\Lambda}) = \\
&\sum_k \mathrm{Tr}\left(\mathbf{W}_k(\mathbf{I}_{N_{bs}} + \lambda_1\mathbf{I}_{N_{bs}} + \sum_{i\neq k}(\lambda_{3,i}\mathbf{H}_i) - \frac{\lambda_{2,k}\mathbf{H}_k}{I_{ue}+\sigma_k^2}\right. \\
&\left. + \mathbf{Q}_{e,k}\mathbf{L}_{1,k}\mathbf{Q}_{e,k}^H + \sum_{i\neq k}(\mathbf{Q}_{e,i}\mathbf{L}_{2,i}\mathbf{Q}_{e,i}^H) - \mathbf{V}_k)\right) \\
&- \sum_k \lambda_{3,k} I_{ue} - \lambda_1 p_{bs} + \sum_k \lambda_{2,k}\eta_k^\star \\
&- \sum_k \mathrm{Tr}\left(\mathbf{L}_{1,k}\overline{\mathbf{S}}_{e,k,1}(\varphi_{e,k}^\star,\vartheta_{e,k})\right) - \sum_k \mathrm{Tr}\left(\mathbf{L}_{2,k}\overline{\mathbf{S}}_{e,k,2}(\rho_{e,k})\right) \\
&- \sum_k \zeta_{1,k}\theta_{e,k} - \sum_k \zeta_{2,k}\rho_{e,k}.
\end{aligned}
\tag{37}
$$

Now, we can use this Lagrangian expression to use the stationary and complementary slackness KKT conditions stated before. By combining both of them, we reach the following expression:

$$\mathbf{X}_k \mathbf{W}_k = \frac{\lambda_{2,k} \mathbf{H}_k}{I_{ue} + \sigma_k^2} \mathbf{W}_k, \qquad (38)$$

where we have defined $\mathbf{X}_k \triangleq \mathbf{I}_{N_{bs}} + \lambda_1 \mathbf{I}_{N_{bs}} + \sum_{i \neq k} (\lambda_{3,i} \mathbf{H}_i) + \mathbf{Q}_{e,k} \mathbf{L}_{1,k} \mathbf{Q}_{e,k}^H + \sum_{i \neq k} (\mathbf{Q}_{e,i} \mathbf{L}_{2,i} \mathbf{Q}_{e,i}^H)$. By looking at this definition of $\mathbf{X}_k$ we clearly see that it is a positive semidefinite matrix (*i.e.,* $\mathbf{X}_k \succeq 0$), and this means that Rank($\mathbf{X}_k$) $= N_{bs}$. Then, by using (38), we have that Rank($\mathbf{W}_k$) = Rank($\mathbf{X}_k \mathbf{W}_k$) = Rank($\frac{\lambda_{2,k} \mathbf{H}_k}{I_{ue} + \sigma_k^2} \mathbf{W}_k$) ≤ min{Rank($\frac{\lambda_{2,k} \mathbf{H}_k}{I_{ue} + \sigma_k^2}$),Rank($\mathbf{W}_k$)} = min{Rank($\mathbf{H}_k$),Rank($\mathbf{W}_k$)} = min{Rank($\mathbf{h}_k \mathbf{h}_k^H$),Rank($\mathbf{W}_k$)} = min{1,Rank($\mathbf{W}_k$)}. This result proves that $\mathbf{W}_k$ will be always a rank-one matrix.

The conclusion behind this proof is that by using SDP and defining the matrix as Hermitian positive semidefinite we can always construct a rank-one solution for $\mathbf{W}_k$. As we have a convex problem in (32), we might directly obtain an optimal solution which will already be rank one. However, in the case that more than one solution exists, by following Theorem 1 we make sure to find the rank-one solution.

4. Deep learning-based resource allocation

As explained in Section 1.1, a deep learning approach can be used in our problem to obtain a close-to-optimal solution without solving a complex optimization problem accurately every time that the resource allocation has to be made. It is important because the users' CSI and the uncertainty of the eavesdroppers' CSI change fast and are unlikely to repeat in future time slots. Then, it is a good approach to obtain a solution close to the optimal one in a way where we reduce the response time or latency compared to the traditional optimization approaches. To do that, the learning system must take into account information about the current scenario bit also results achieved in previous time slots that had similar conditions.

Our deep learning approach seeks to combine the maximization study proposed in Section 3 with the so-called classification neural networks. We propose two different types of neural networks which are going to predict the beamforming that maximizes the global secrecy rate considering all the users. Note that, to achieve the global maximization, the beamforming corresponding to every user depends both on the position of other legitimate users and the position of eavesdroppers. Then, the challenge is to determine the suitable parameters (*i.e.,* inputs of the learning system) that are useful to decide every beamforming strategy. These parameters must provide enough information to describe the global scenario.

The prediction obtained by the learning system will allow to avoid rerunning the convex optimization algorithm and, instead, use the knowledge obtained from historical data to allocate the resources in new scenarios. This is extremely useful when dealing with dynamic scenarios where users keep moving fast. Following this idea, the proposed learning system will predict the beamforming for every antenna at the BS transmitting information to every user. Our proposal is to consider that we depart from an initial scenario where the resource allocation has already been done and is known. Sometime later, a user in the scenario decides to move and there is the need to recompute the beamforming that achieves secrecy performance. By considering the resource allocation of the initial scenario, we have information of the position of all the users in the network and it can be interpreted as having a signature of this departing scenario. In other words, it is a way of reducing the large amount of sample data that would be necessary if we considered the CSI of every user and eavesdropper instead.

4.1. Input layer

As mentioned, we propose two types of neural networks: one to predict the beamforming for the user that has decided to move (from now on defined as class A neural networks) and the other for the users that remain static (defined as class B neural networks). Notice that we are going to predict the beamforming (magnitude and phase) of every signal sent by the BS, so we need to consider and predict every antenna at the BS and legitimate user independently. Additionally, to achieve faster convergence during training with the gradient descent algorithm, we propose a symmetric feature scaling for the inputs (rescaling its values to the interval $[-1,1]$).

In our work, when dealing with complex parameters the real and the imaginary part are going to be considered as independent inputs. Following this consideration, the input parameters of a class A network that is going to be used to predict the beamforming of a specific antenna will consist of: i) the initial scenario's beamforming for the user that is going to move (real and

imaginary part for the considered antenna) $\Re\{w_{l,k}^{ini}\}$ and $\Im\{w_{l,k}^{ini}\}$, ii) the interference levels experienced by every user in the initial scenario $I_{ue_k}^{ini}$, and iii) the new CSI (real and imaginary part) of the user that is going to move $\Re\{h_{l,k}^{new}\}$ and $\Im\{h_{l,k}^{new}\}$. As an example, in a scenario with 10 legitimate users let us say that we want to predict the beamforming of one of the antennas at the BS for the dynamic user. Then, in this case we would have 14 different input nodes in the class A neural network used to predict the beamforming of the considered antenna: the two inputs regarding the initial beamforming allocation, ten interference levels and two CSIs.

Regarding the class B neural network, the input nodes are similar but they also need to consider the new CSI of the user that is moving. The reason is that the optimal beamforming for every static user depends on the new position of the dynamic user. In this case, the inputs will be: i) the beamforming of the initial scenario for the considered static user (real and imaginary part for the considered antenna and considering this user) $\Re\{w_{l,k,s}^{ini}\}$ and $\Im\{w_{l,k,s}^{ini}\}$, ii) the interference levels experienced by every user in the initial scenario $I_{ue_k}^{ini}$, iii) the CSI of the considered static user (real and imaginary part) $\Re\{h_{l,k,s}\}$ and $\Im\{h_{l,k,s}\}$, and iv) the new CSI of the user that is moving (real and imaginary part) $\Re\{h_{l,k',d}^{new}\}$ and $\Im\{h_{l,k',d}^{new}\}$. Consequently, compared to the class A neural network, the class B neural network will have two more inputs no matter the number of legitimate users. The inputs for each type of neural network are depicted in Figure 10 and Figure 11.

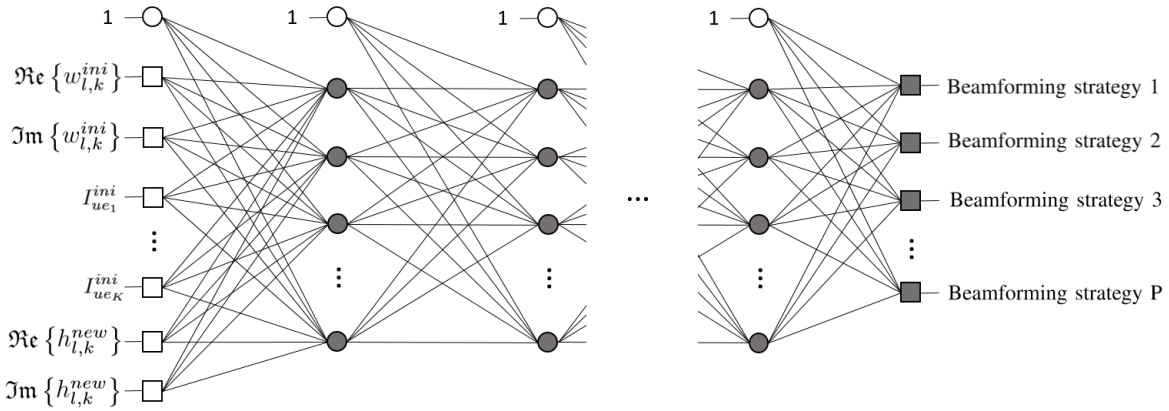


Figure 10 Block diagram of the proposed class A neural network used in the learning system for a dynamic user. It considers a scenario with K legitimate users and predicts the beamforming strategy of the base station's antenna l among the P strategies in the beamforming codebook.

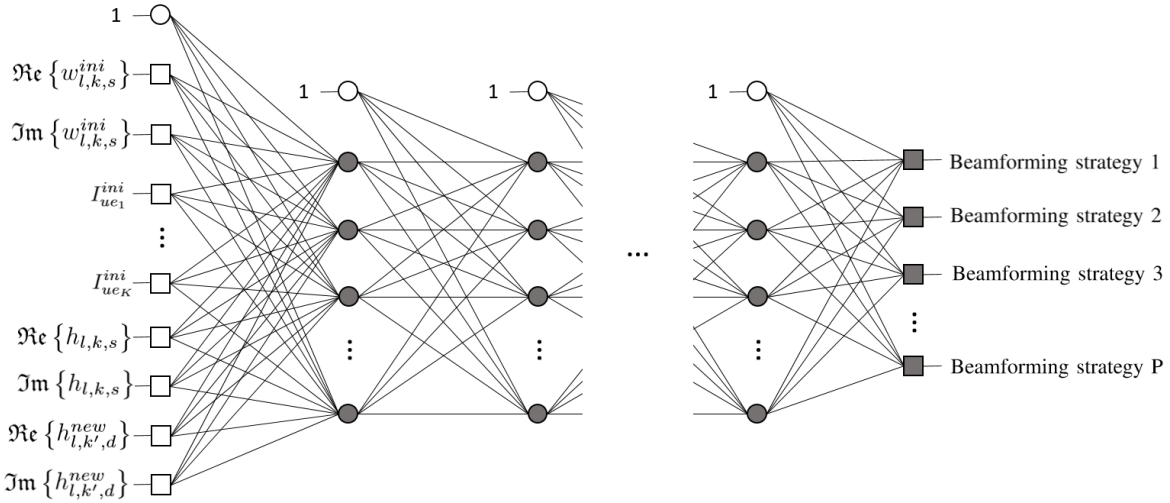


Figure 11 Block diagram of the proposed class B neural network used in the learning system for a static user.

4.2. Hidden layers

Regarding the hidden layers, we propose a fully connected layer architecture and using ReLu as activation functions. This type of activation function is widely used in deep learning methods [38]. The number of hidden layers and nodes in each hidden layer directly impacts the learning system's performance and has to be determined experimentally as it will be showed later in the document in the results part.

4.3. Output layer

As we propose a classification deep learning method, the output of our learning system is going to be a class. Each class is going to correspond to a beamforming strategy, which is the predicted beamforming for the considered antenna and user. Thus, to make the classification possible, the number of output nodes has to be equal to the number of possible beamforming strategies. The considered possible beamforming strategies are going to be contained in what we call the beamforming codebook, which is formed by listing the different beamforming strategies contained in our training set. Notice that in real environments, where the training set may be very large, to avoid storage issues a good approach may be clustering the different beamforming strategies prior to creating the beamforming codebook. This will lead to discovering underlying structure in the data and reducing the dimensionality.

Our model is going to choose the best beamforming strategy (*i.e.,* class) that corresponds to the input parameters fed into the neural network. To obtain this class we use a softmax activation function and therefore obtain the probabilities for each output class. Additionally, as we have to predict a beamforming for every antenna and legitimate user, in a scenario with K legitimate users and N_{bs} antennas we will need $K \cdot N_{bs}$ neural networks for prediction purposes. From these $K \cdot N_{bs}$ neural networks, N_{bs} neural networks will be class A and $(K-1) \cdot N_{bs}$ class B.

4.4. Creating the training set

The strategy followed to train the proposed neural networks is to use supervised learning. Therefore, prior to train the network we need to obtain a training set where each training sample is labeled with the corresponding output class. However, note that each training sample is

characterized by the corresponding group of input features. Additionally, our proposed learning system is going to predict the resulting beamforming strategy after a user decides to move in a given initial scenario. Then, to create the training set, the first steps are to generate random initial scenarios. After that, for each of them, we need to generate random moving possibilities for the dynamic user.

For a given total number of legitimate users *K* in the scenario we are going to generate N_{ds} different initial scenarios and, in each of them, generate N_{mov} different movement possibilities for the dynamic user. This is, for the N_{ds} different initial scenarios, we need to randomly generate all the downlink channels following the statistical distribution detailed in Section 3.2.1 and solve the convex optimization problem after setting all the physical layer parameters. From the solutions obtained in each initial scenario, we store in the training set dataset the initial scenario's parameters that will be needed for training purposes (*i.e.,* initial beamforming strategies and initial interference levels for every user). After this is done, for all the N_{ds} we need to generate N_{mov} new scenarios that would be obtained if a user decided to move. This is to generate N_{mov} different CSIs for the dynamic user and store them in the training dataset too as this is information that will be used as inputs of the neural networks as explained in Section 4.1 and in Figure 10-Figure 11.

Once the new modified scenarios are generated, the next step is to recompute the convex optimization problem to find the new beamforming strategies for each antenna and user. These allocations are going to be stored because they are going to be used as the labels of the dataset samples used in the supervised learning. In that way, we are going to generate one dataset for every antenna at the BS and legitimate user. This is, in a case with $N_{bs} = 10$ and $K = 10$ we will generate 100 databases for the training set.

4.5. Training process

The training of the neural networks is going to be done following a supervised learning approach and considering early stopping as a way to prevent underfitting and overfitting. To learn the weights, the cost function used is cross-entropy and the stochastic gradient descent algorithm is used to find the optimal solution considering this cost function. Additionally, as we are using ReLu activation functions, a good way to initialize the weights is by using the He initialization. To achieve good performance, the tuning of the hyperparameters has been done experimentally until the desired performance has been achieved. The tuning included finding the suitable number of nodes at each hidden layer, the number of hidden layers, the suitable learning rate and number of epochs. These parameters were essential to avoid underfitting when working with large training sets, as more capacity was required. On the other hand, to avoid overfitting, dropout layers are used in our architecture with a probability of 0.5 to remove the hidden units. An L2 regularization constant is also considered to this end.

4.6. Assessing the prediction

Once the learning system predicts the beamforming allocation for the desired scenario, there is an algorithm that makes sure that this solution satisfies power and interference constraints. First, the beamforming considering all the antennas at the BS has to use a total power that has to be lower or equal than the total available transmitting power. Once this is achieved, the algorithm has to make sure that the interference experienced by the legitimate users is below the level I_{ue}

set by the network operator. To do that, we propose a power reduction technique that, given the predicted solution, gives as output the new beamforming allocation that satisfies all the constraints.

The algorithm scales down the allocated power but keeping the proportions of the initial solution, as changing the proportions would mean arbitrarily obtaining a different solution that will not guarantee secrecy performance. During some iterations, the power of each antenna and for each user is reduced a predefined step (*e.g.,* 0.5% of the initial values) until the available transmitting power is not exceeded. Then, a new predefined step is computed to increase the power of each antenna until achieving desired performance. After the algorithm guarantees not exceeding the available transmitting power, if the interference constraint is not guaranteed in any user the algorithm keeps reducing the transmitted power until all the users have interference levels below the fixed threshold.

To summarize everything, Figure 12 shows the blocks needed to obtain a learning-based resource allocation prediction.

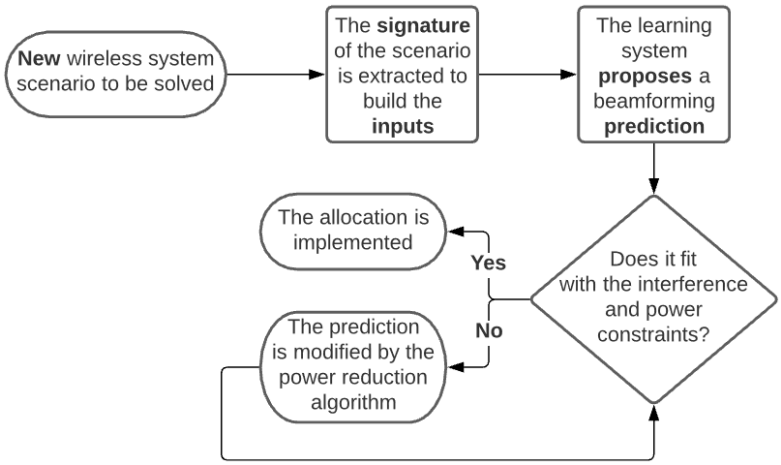


Figure 12 Learning system blocks

5. Results

5.1. Parameters for the simulations

A topology with four nodes (*i.e.,* two legitimate receivers and two eavesdroppers) is considered to simulate and obtain the results in the majority of this section after implementing the solution proposed in Sections 3 and 4. An example of a scenario is given in Figure 13.

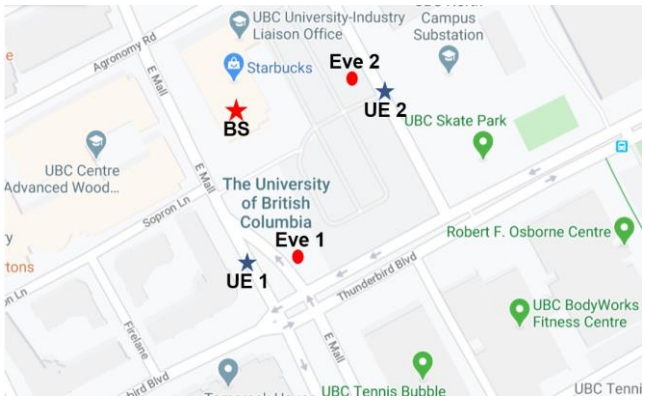


Figure 13 Scenario with 4 nodes at UBC campus

For the depicted scenario, we are considering a multi-antenna BS with two antennas employed for the downlink transmission. As explained in Section 3.1, the legitimate receivers are considered single antenna devices with low computational capabilities while the eavesdroppers are multi-antenna powerful devices. Regarding the physical layer parameters used in the optimization problem, realistic values have been used. First, we assume that the noise power received by each node is the same and equal to $\sigma^2 = -170\ dBm + 10\log_{10}(20 \cdot 10^6\ \text{Hz}) = -97\ \text{dBm}$. The CSI has been simulated following the statistical distribution explained in Section 3.2.1. For the interference bounds, we have a lower bound for the eavesdroppers and an upper bound for the legitimate receivers. As they would be parameters set by the MNOs, to compute each bound we iteratively searched values until we achieved realistic values for the SINR of each node. Then, for the uncertainty radius, we assume that it can be computed as a fraction of the statistical knowledge available at the BS (let's say a 5% of the value). For the available transmitted power at the BS, we assume 23 dBm. Lastly, for the iteration number in the convex system explained in Section 3.2.5, we have set the limit to 50 and for the learning system we set three hidden layers with 100 nodes in each layer and the learning rate was set to 0.001.

5.2. Simple case allocation

To start showing the results with the simplest scenario, let's first show the resource allocation obtained with just one legitimate receiver and eavesdropper. After randomly generating the CSI values and initializing the physical layer parameters, Table 1 summarizes the results obtained. As seen, we can directly obtain the resource allocation after doing the SVD of matrix $\mathbf{W_k}$. In this case, as we can see that the eigenvalue is 1, we can directly take the first column of the first matrix of the decomposition for the resource allocation. From this, we can conclude that to maximize the secrecy rate in this scenario, the legitimate receiver can leverage the channel of the first antenna and this is why most of the power is allocated to it.

CSI legitimate user	$\mathbf{h}_k = \begin{bmatrix} 0.38 + j0.58 \\ 0.40 + j0.02 \end{bmatrix}$
Statistical knowledge for the eavesdropper	$\hat{\mathbf{g}}_{e,k} = \begin{bmatrix} 0.58 + j0.11 \\ 0.93 + j0.73 \end{bmatrix}$
$\mathbf{W}_k$	$\mathbf{W}_k = \begin{bmatrix} 0.75 & 0.26 + j0.35 \\ 0.26 + j0.35 & 0.25 \end{bmatrix}$
Resource allocation	$svd(\mathbf{W}_k) = \begin{bmatrix} -0.87 & 0.50 \\ -0.29 + j0.40 & -0.51 + j0.70 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \cdot \begin{bmatrix} -0.87 & 0.50 \\ -0.29 + j0.40 & -0.51 + j0.70 \end{bmatrix}$

Table 1 Results for the network with two nodes

However, before starting to obtain more complex results, we need to provide results showing that the assumption made in Section 3.2.5 to apply the Taylor series approximation holds. We said that the SINR at the eavesdroppers would be very low and almost zero, something that Figure 14 shows. We simulated 20000 random scenarios and obtained the cumulative distribution function for the SINR values obtained in them.

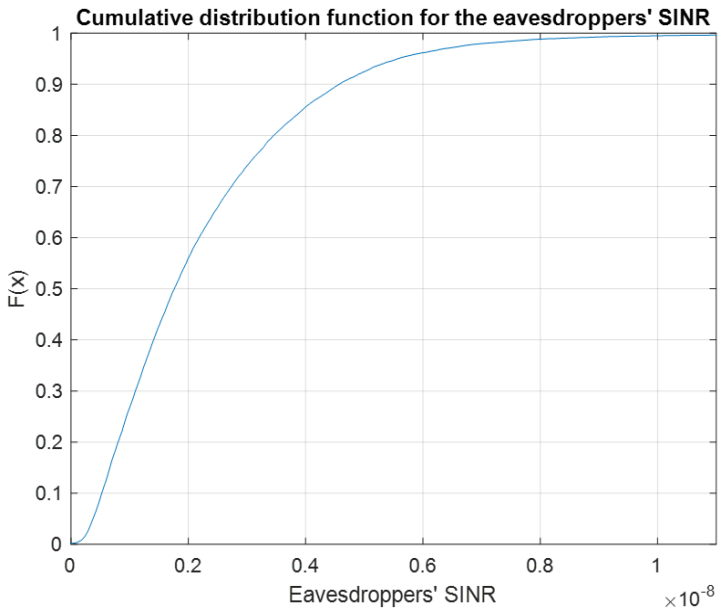


Figure 14 Cumulative distribution function for the eavesdroppers' SINR

5.3. Obtaining the dataset

Once we checked that the convex optimization-based resource allocation was providing reliable results, we started working on the training set for the learning system. The process followed is explained in Section 4.4, but here we include some figures of the process. To obtain a sufficient training set, and following the terminology used in Section 4.4, we set $N_{ds} = 320$ and $N_{mov} = 154$. This means that we simulated 49280 scenarios (*i.e.,* 320x154) for training purposes. As we were considering two legitimate users in the network and two antennas at the BS, for each of these scenarios we had four beamforming values that were used as labels of the two class A and two class B neural networks:

$w_{1,1}, w_{1,2}, w_{2,1}$ and $w_{2,2}$. Figure 15 shows the obtained beamforming allocations for the second antenna and referring to the dynamic user.

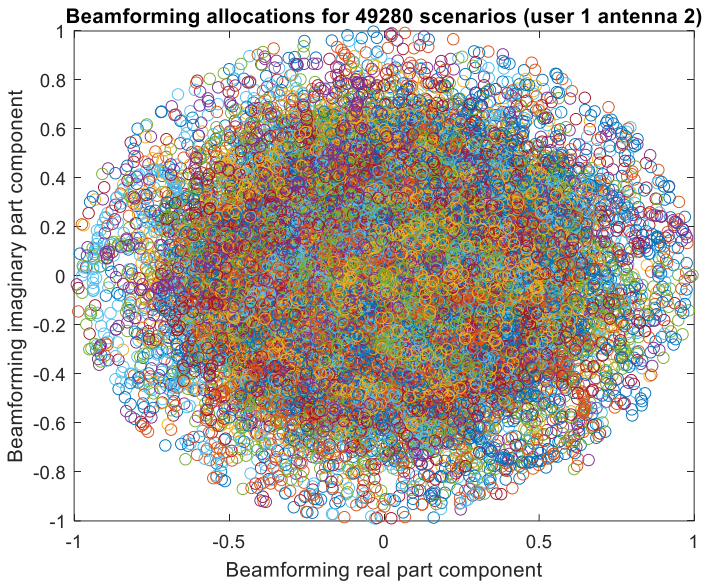


Figure 15 Beamfoming allocations for a specific user and antenna for 49280 scenarios

Then, each of these allocations is going to be considered as a class for the classification neural network of user 1 and antenna 2. For the simplicity of the rest of this subsection, let's consider a case with $N_{ds} = 20$ and $N_{mov} = 20$ (*i.e.,* 20x20 training set) and imagine that we wanted to apply the k-means algorithm for clustering the classes. This scenario is depicted by Figure 16 and Figure 17.

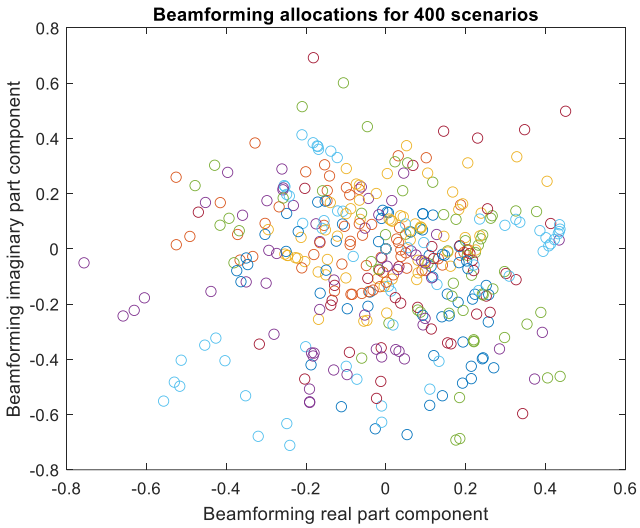


Figure 16 Beamforming allocations for the 20x20 case

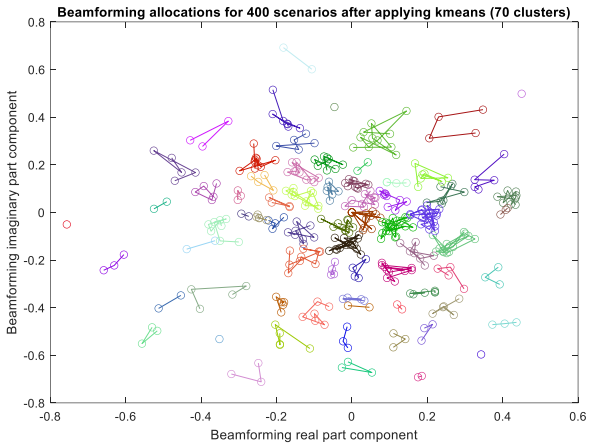


Figure 17 Clustered beamforming allocations for the 20x20 case

With these labels for the supervised learning and the information saved to build the inputs of the learning system, we could build the dataset to train the network. Following the structure for the inputs explained in Section 4.1, some entries of the clustered dataset (fixing N_{ds} and for five different N_{mov}) are depicted in Table 2, where the last column corresponds to the class number obtained by the k-means algorithm. Notice that scenario 1 and scenario 5 are classified with the same class number because of the similarity of their beamforming allocations as seen in Figure 18.

	1	2	3	4	5	6	7
1	0.0143	-0.3579	0.2943	0.2779	-1.8535	0.2186	65
2	0.0143	-0.3579	0.2943	0.2779	0.8655	-1.1149	40
3	0.0143	-0.3579	0.2943	0.2779	1.6173	-1.1271	15
4	0.0143	-0.3579	0.2943	0.2779	0.2405	0.9931	50
5	0.0143	-0.3579	0.2943	0.2779	0.7414	2.4739	65

Table 2 Training set entries for five different movements

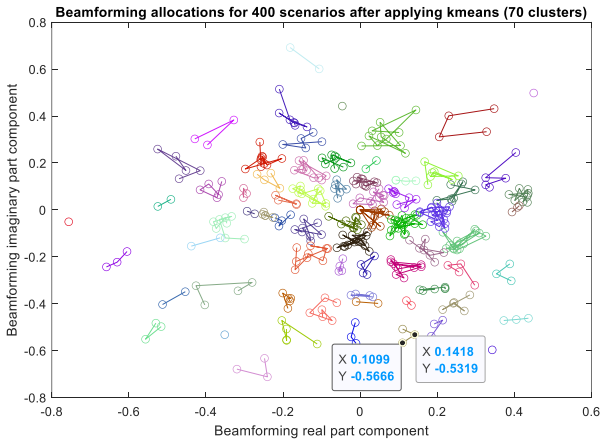


Figure 18 Information about two samples clustered with the same class in the beamforming codebook

To assess the impact of clustering in the performance of our learning system we decided to generate a 60x60 training set and use it in two ways: with and without clustering. The beamforming allocations for a given user of this training set is depicted in Figure 19 and Figure 20. After tuning the hyperparameters of the neural networks for the new training set, we trained the

networks and predicted the beamforming allocations to maximize the secrecy rate in the same 30 random scenarios. Results showed that the non-clustered training set achieved a 13% performance increase compared to the clustered training set.

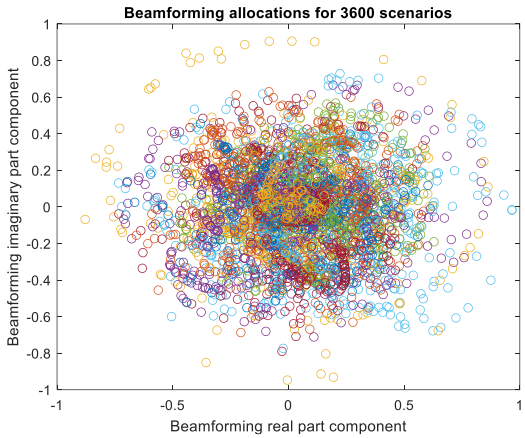


Figure 19 Beamforming allocation for the 60x60 case (no clustering)

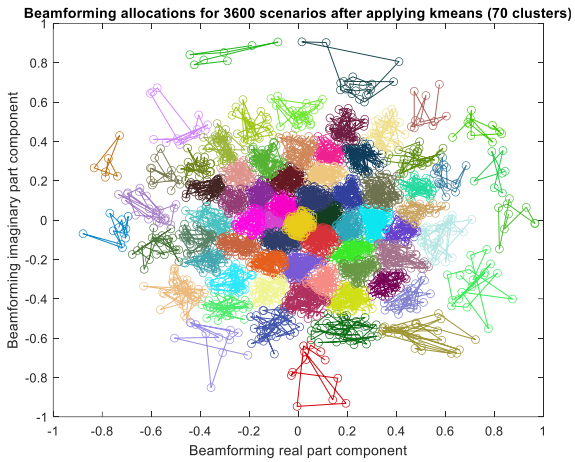


Figure 20 Beamforming allocation for the 60x60 case (with clustering)

5.4. Normalized secrecy performance and power efficiency

This subsection assesses the performance of the proposed study. First, we want to show the results obtained with our optimization and learning study and compare it with a random allocation approach. By doing this, we are going to have a clear idea of the performance improvement that we can achieve by using each of the proposed tools. With these results, the user can understand the existing trade-off between achieving optimal performance and having low computational cost.

Figure 21 shows the performance achieved by each algorithm in 60 randomly generated scenarios when considering a training set with $N_{ds} = 100$ and $N_{mov} = 100$. Knowing that the convex-based allocation is always going to provide the best secrecy performance, we normalized the secrecy rate achieved by each algorithm taking as reference the one obtained by the convex allocation. In this scatter plot, we depict in the x-axis the amount of power used in the resource allocation of each of the 60 random scenarios. As seen in the scatter plot, the convex-based resource allocation always uses all the available transmitting power and achieves the best

performance. This makes that all the 60 points corresponding to the convex allocation of the random scenarios are overlapped in the same position of the graph (top-right point).

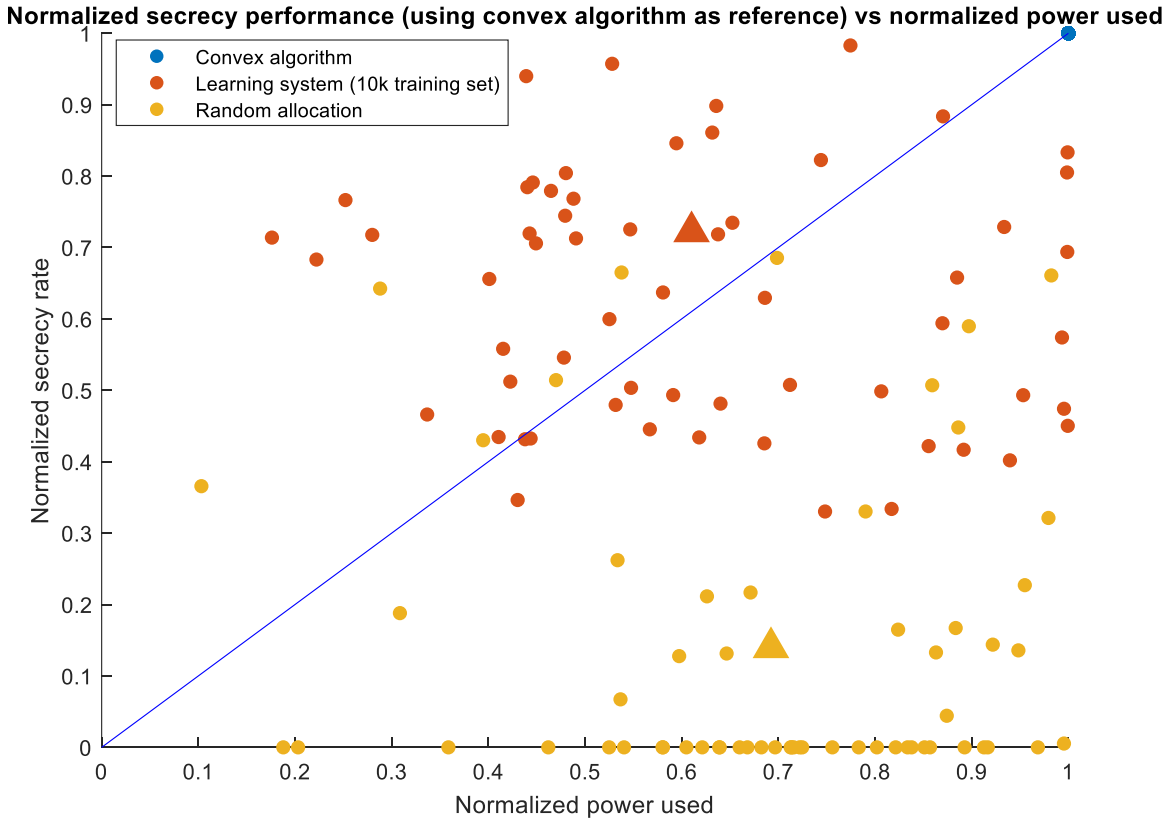


Figure 21 Scatter plot showing the normalized secrecy performance for the convex problem-based allocation, the learning system prediction and the random allocation for 60 random scenarios.

On the other hand, we see that for the learning system and the random allocation the amount of power used varies from case to case. In the learning system's case, the average performance is lower than the convex approach but much higher than the random allocation. However, by using the learning approach we achieve the highest power efficiency if we define it as the normalized secrecy rate over the normalized power used. We can check that by comparing the orange triangle (mean point for the learning system's scenarios) with the blue line going from (0,0) to (1,1) that would correspond to points with power efficiency equal to one. This means that the learning approach is the one that can use less power to achieve good secrecy performance, as seen in Figure 22.

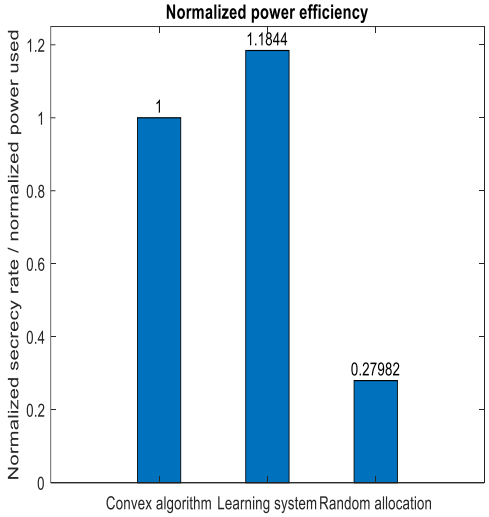


Figure 22 Bar graph showing the average normalized power efficiency considering the 60 random scenarios.

From these results we can extract that the best approach to compute the resource allocation depends on the particular scenario that we have. Starting with the convex optimization-based resource allocation, it would be interesting to use it when dealing with static scenarios. This is because the resource allocation will be the same for the time that the users remain static, so it is worth computing an optimal allocation that provides the best performance. Additionally, the convex approach might be useful in cases where the main concern is achieving the highest possible level of secrecy in the communication. An example of this would be the IoT emergency or safety use cases.

On the other hand, in cases where the channel is changing fast (*e.g.,* inside vehicles or with moving obstacles) we may not have time to compute the optimal resource allocation before the channels change. In this case the best approach is obtaining a learning-based prediction. We can obtain this prediction almost instantaneously just by feeding the input parameters to the learning system and still achieve a performance much higher than the random allocation. Furthermore, this learning-based resource allocation can also be interesting in cases where high power efficiency is required. This is, in cases where the available transmitting power is limited, good secrecy performance can still be achieved while using less power. An example of this power-limited scenarios might be when frequency reuse is expected in adjacent cells. In this case, low transmitting power is desired to avoid inter-cell interference.

5.5. Focusing on the training set size

In this subsection we focus on the learning system to show the correlation between the performance achieved and the training set size. As our learning system is based on classification neural networks, the secrecy performance achieved by our predicted resource allocation will directly depend on the size of the training set used for the supervised learning process. Then, in our study we simulated a maximum of 49280 scenarios and used them to obtain the training set. But to show how the performance evolved with the training set size we decided to create sub training sets with the following sizes: 7k, 14k, 21k, 28k, 35k, 42k and 49k samples. After training the networks with the previous sizes of training sets we tested the performance achieved by each of them in terms of normalized secrecy rate and power efficiency. The results are included in Figure

23. To obtain the results for each sub training set, we tested the trained networks with 60 randomly generated scenarios. Then, we averaged the normalized secrecy rate and power efficiency achieved in each of these 60 scenarios and plotted them as a point in the previous plot.

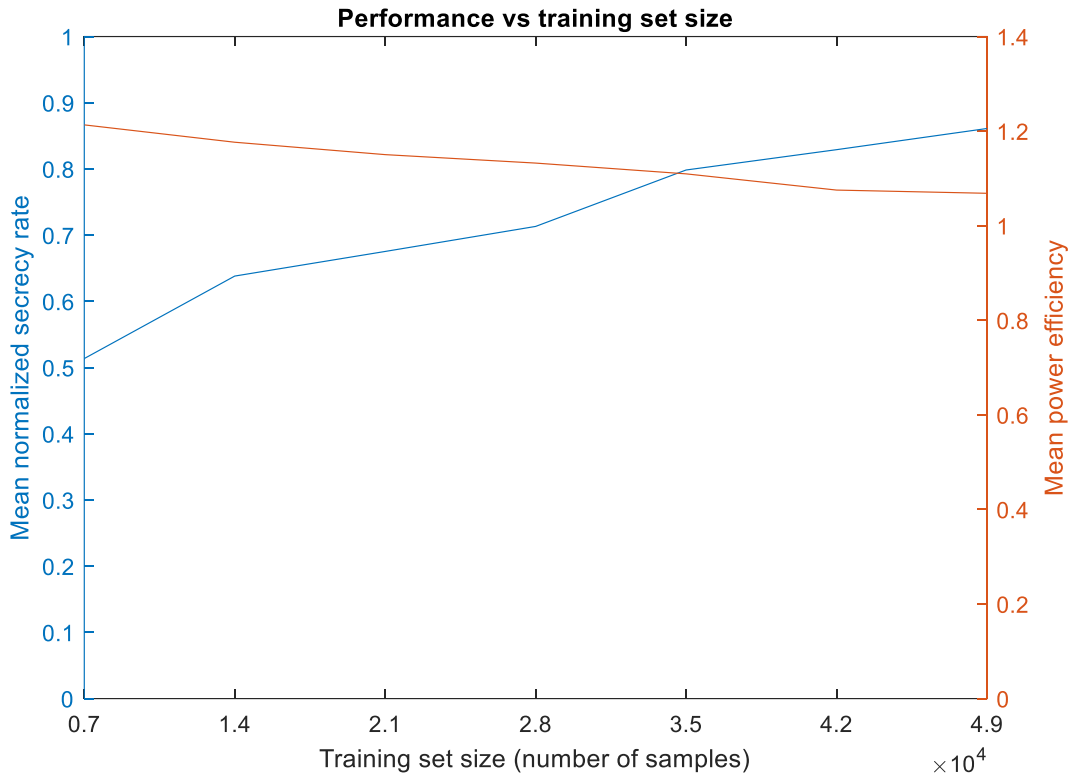


Figure 23 Performance achieved as a function of the training set size

Figure 23 shows two main results: the secrecy rate performance increases as the number of samples in the training set increases and the power efficiency decreases as the number of samples increases. The first result was expected before running the simulations, but the second result was not. But after analyzing this, we realized that in fact the two results are linked. When the number of samples in the training set increases, the accuracy of the classification also increases and this means that the solution provided by the learning system is more similar to the solution proposed by the convex algorithm. Thus, as in Figure 21 we saw that the power efficiency was lower for the convex allocation, if we now have learning-based predictions that are more similar to the actual convex-based allocations we will obviously have a decrease in the power efficiency. To clearly show this idea we created Figure 24 and Figure 25. They are showing the same results that Figure 21 and Figure 22 but comparing the results obtained with the 10k and 20k training sets and removing the random and convex-based allocation.

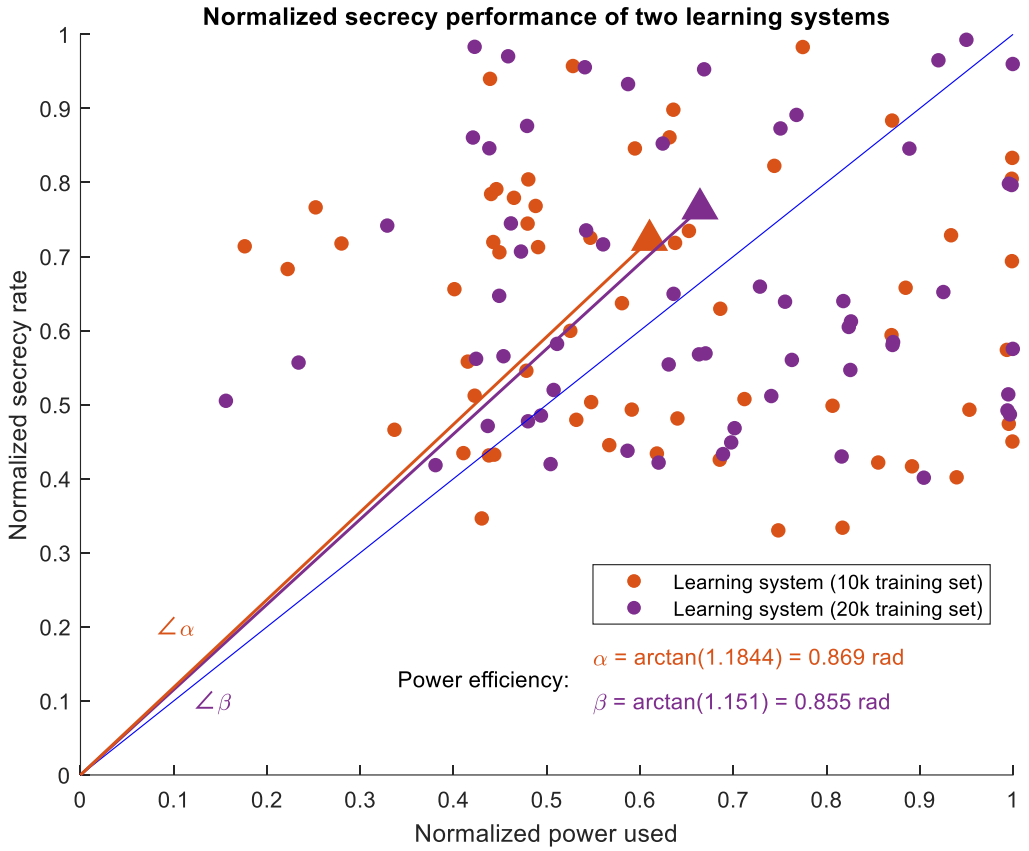


Figure 24 Scatter plot showing the normalized secrecy performance for two learning systems in 60 random scenarios

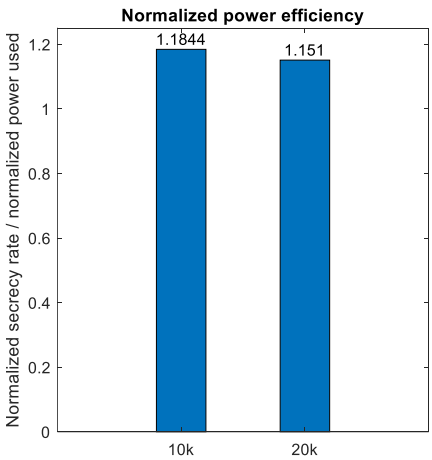


Figure 25 Bar graph showing the average normalized power efficiency in two learning systems

As seen in the previous two figures, the learning system trained with 20k scenarios achieves higher secrecy rate and lower power efficiency. If we take a look to the top-right part of Figure 24, we see that more purple samples are close to the (1,1) point corresponding to the convex allocation as seen in Figure 21. Then, we checked that by increasing the training set size more samples plotted in the scatter plot are going to tend to the (1,1) optimal solution of the convex problem. As observed in the values of the angles α and β of Figure 24 or in Figure 25, there is a significant difference in power efficiency but just 10k samples difference in the training set. The

angles are defined by the line that goes from (0,0) to the mean point of each training set and the horizontal axis.

5.6. Influence of users' speed in our study

Finally, we would want to show the impact of users' speed in our study. A question that may arise to the reader is how we can take advantage from knowing if we are dealing with a fast or a slow moving user. Regarding the convex-based resource allocation there is no way of using this information, but the learning approach can give us the possibility to leverage this information. Until now we trained the neural networks with training sets that were obtained using a number of different moving possibilities N_{mov}. But we know that a slow moving user will experience soft changes in the slow fading part of the channel, meaning that the variations in the channel are going to be much lower. Then, instead of using a training set with wide possibilities of CSIs we could just focus on training the networks with a smaller range of CSI values in the training set. To do that, we have regenerated our training set but assuming two different channel model with much lower variance. We propose using as channel models the two following statistical distributions: $\mathcal{CN}(0,0.2)$ and $\mathcal{CN}(0,0.02)$. The second one represents a scenario with slower users than the first one but both are for slower users compared to the original channel model used in the rest of the sections of the document. Then, with these new training sets we wanted to show the performance of the learning systems as done in Figure 23:

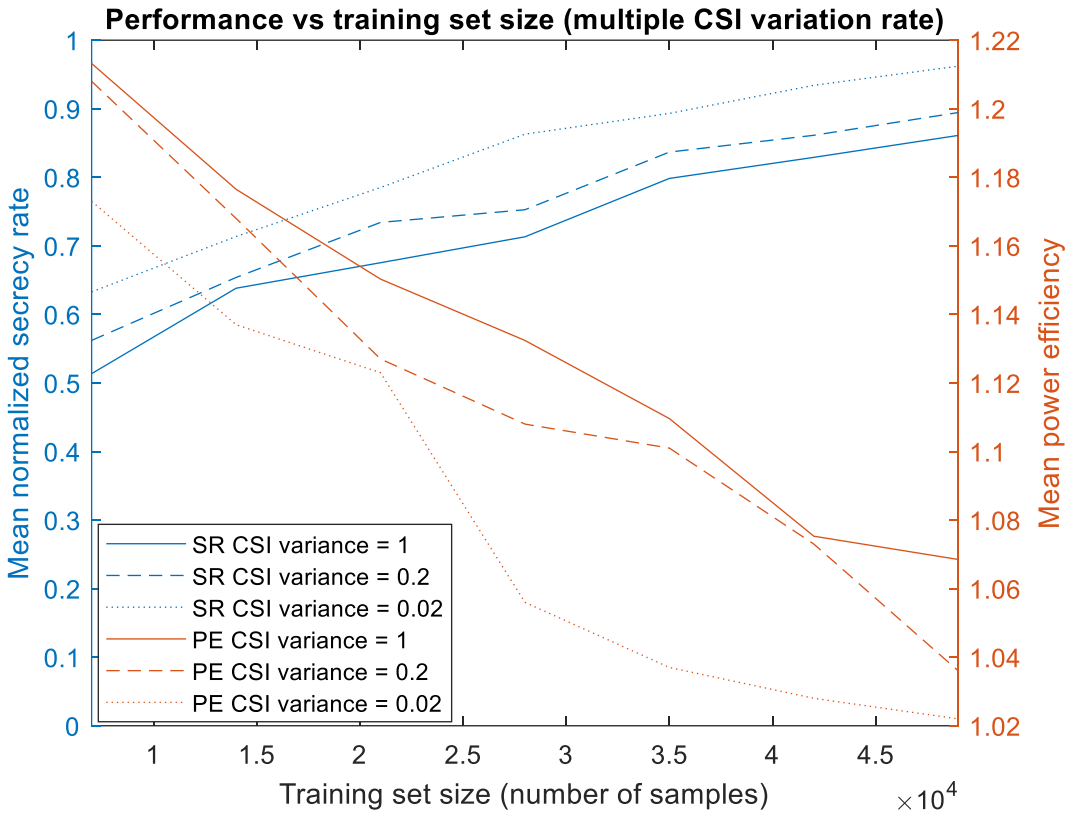


Figure 26 Performance achieved as a function of the training set size for different user speeds

From Figure 26 we confirm that the performance of the learning system in terms of secrecy rate improves when dealing with scenarios with slower users. This is why the secrecy rate for the

case with smallest variance is the one with the best performance and the one with the highest variance is the worst. In addition, when we look into the power efficiency obtained, we see that the behavior is similar to what we discovered in Section 5.5. This is, when we have a more accurate prediction (*i.e.*, more similar to the convex allocation) the power efficiency decreases. Then, it makes sense that the case with variance equal to 1 provides the highest power efficiency while the case with variance equal to 0.02 has the lowest. It is worth mentioning that, by using Figure 26, the network operator can easily identify the training set size needed to achieve a given secrecy rate. By using the minimum training set size required, the desired secrecy rate is achieved and the power efficiency is maximized.

6. Conclusions and future development

This project sought to provide different approaches to achieve global secrecy performance in the TDD-based downlink transmission of the 5G wireless heterogeneous scenario. Our work has been done considering the computational constraints derived from low complexity IoT devices, the multi-antenna architecture of nodes and the eavesdroppers' unwillingness to provide channel state information to the base station. Additionally, different tools have been designed to address either the static or dynamic wireless environment.

First, the wireless system has been modelled by using mathematical formulation. A set of legitimate receivers and multi-antenna eavesdroppers have been considered and the mathematical notation allowed us to find expressions for their received signals, signal-to-interference-plus-noise ratios or achieved data rates. We modelled the eavesdroppers' unwillingness to reveal their existence by introducing an uncertainty model associated with their CSI. After all this initial modelling, we first proposed a convex-optimization based resource allocation using physical layer security concepts to maximize the global secrecy rate of the considered scenario under a transmit power constraint. As the initial problem was not convex, we detailed the relaxation techniques followed to obtain the resulting convex optimization problem. These techniques included: i) introducing an interference decoupling that bounded the interference perceived by legitimate receivers and eavesdroppers, ii) using the so-called S-Procedure to remove infinitely inequality constraints introduced by the continuity of the space defining the eavesdroppers' CSI uncertainty region, and iii) applying the Taylor series approximation theory to propose an iterative algorithm that approximates the signal-to-interference-plus-noise ratios of the eavesdroppers. We also provided the study to convert the relaxed convex problem into something that can be solved using convex optimization solvers such as CVX. This conversion required reformulation and adding constraints as detailed.

After we detailed this convex optimization-based resource allocation, we introduced deep learning to our study. The need to do it was because dynamic environments could abruptly change the CSI and the convex approach could not deal with it because there might be no time to compute the convex-based solution. Then, the approach proposed is a learning system that uses the convex optimization study during training. Our learning system is based on classification neural networks that will predict the best resource allocation in terms of secrecy performance when a set of inputs are fed into the system. As detailed, the inputs of the networks depend on factors such as the movement of the user or the number of legitimate receivers in the scenario. We detailed the architecture of our system, including the input layer, the hidden layers and the output layer for each of the two types of neural networks proposed. After that, we explained more practical aspects such as how to obtain the training set used in the supervised learning process or how to perform this training process. Then, we discussed how to assess the obtained prediction when dealing with transmitting power limitations or interference constraints.

In the results part we showed that the project fulfilled the objectives set at the beginning. We first started by showing how the convex optimization-based resource allocation can find the optimal beamforming strategy to maximize secrecy performance in simple scenarios. After this was done, we used this approach to show that our assumptions made during relaxation steps were correct. Then, we gave examples of clustered and not clustered beamforming codebooks obtained

during our study and we provided details about the datasets used during training of the learning system. Using all this led us to results showing that both of the two tools proposed in our study achieve much better performance than a random approach. In addition, we gave a discussion about the possible use cases (*e.g.* static vs dynamic environments, small cells with frequency reuse or high performance cases) of each of the two approaches and gave an analysis in terms of power efficiency. This showed us that, while the convex optimization-based allocation achieves optimal secrecy performance, the learning approach might be very interesting in terms of power efficiency.

More detailed results were given regarding the correlation between the training set size and the performance of the learning system. In this way, we showed the performance achieved by using both small and large training sets and the impacts that this has in the power efficiency. We showed that results highlight two behaviors: i) the secrecy performance increases when the training set increases, and ii) the power efficiency decreases as the training set increases. This is due to the asymptotic behavior that the learning system has to the convex approach with large training sets. Once this was done, we provided a study about the influence of users' speed in the learning system's performance.

Additional work might derive from the proposed study. Regarding the convex-based resource allocation, techniques such as injecting artificial noise could be added to the problem to achieve better secrecy performance. Regarding the learning system, further improvements could be implemented by adapting to this new convex problem and changing the inputs of the neural networks. To determine the best possible inputs, one option is to perform a deep study using the Lasso regression tool to select them.

Bibliography

[1] A. Hyadi, Z. Rezki and M. Alouini, "An Overview of Physical Layer Security in Wireless Communication Systems With CSIT Uncertainty," in IEEE Access, vol. 4, pp. 6121-6132, 2016, doi: 10.1109/ACCESS.2016.2612585.

[2] A. Yener and S. Ulukus, "Wireless Physical-Layer Security: Lessons Learned From Information Theory," in Proceedings of the IEEE, vol. 103, no. 10, pp. 1814-1825, Oct. 2015, doi: 10.1109/JPROC.2015.2459592.

[3] J. Zhu, R. Schober and V. K. Bhargava, "Linear Precoding of Data and Artificial Noise in Secure Massive MIMO Systems," in IEEE Transactions on Wireless Communications, vol. 15, no. 3, pp. 2245-2261, March 2016, doi: 10.1109/TWC.2015.2500578.

[4] *S. Goel and R. Negi, "Guaranteeing Secrecy using Artificial Noise," in IEEE Transactions on Wireless Communications, vol. 7, no. 6, pp. 2180-2189, June 2008, doi: 10.1109/TWC.2008.060848.*

[5] *A. Ijaz et al., "Enabling Massive IoT in 5G and Beyond Systems: PHY Radio Frame Design Considerations," in IEEE Access, vol. 4, pp. 3322-3339, 2016, doi: 10.1109/ACCESS.2016.2584178.*

[6] M. Mohri, A. Rostamizadeh, and A. Talwalkar, "Foundations of Machine Learning". Cambridge, MA, USA: MIT Press, 2012.

[7] T. O'Shea and J. Hoydis, "An Introduction to Deep Learning for the Physical Layer," in IEEE Transactions on Cognitive Communications and Networking, vol. 3, no. 4, pp. 563-575, Dec. 2017, doi: 10.1109/TCCN.2017.2758370.

[8] S. Yousefi, H. Narui, S. Dayal, S. Ermon and S. Valaee, "A Survey on Behavior Recognition Using WiFi Channel State Information," in IEEE Communications Magazine, vol. 55, no. 10, pp. 98-104, Oct. 2017, doi: 10.1109/MCOM.2017.1700082.

[9] C. Huang, C. Chiang and Q. Li, "A study of deep learning networks on mobile traffic forecasting," 2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC), Montreal, QC, 2017, pp. 1-6, doi: 10.1109/PIMRC.2017.8292737.

[10] L. Fernández Maimó, Á. L. Perales Gómez, F. J. García Clemente, M. Gil Pérez and G. Martínez Pérez, "A Self-Adaptive Deep Learning-Based System for Anomaly Detection in 5G Networks," in IEEE Access, vol. 6, pp. 7700-7712, 2018, doi: 10.1109/ACCESS.2018.2803446.

[11] A. Vora, P. Thomas, R. Chen and K. Kang, "CSI Classification for 5G via Deep Learning," 2019 IEEE 90th Vehicular Technology Conference (VTC2019-Fall), Honolulu, HI, USA, 2019, pp. 1-5, doi: 10.1109/VTCFall.2019.8891133.

[12] Q. Mao, F. Hu and Q. Hao, "Deep Learning for Intelligent Wireless Networks: A Comprehensive Survey," in IEEE Communications Surveys and Tutorials, vol. 20, no. 4, pp. 2595-2621, Fourthquarter 2018, doi:10.1109/COMST.2018.2846401.

[13] G. Han, L. Xiao and H. V. Poor, "Two-dimensional anti-jamming communication based on deep reinforcement learning," 2017 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), New Orleans, LA, 2017, pp. 2087-2091, doi: 10.1109/ICASSP.2017.7952524.

[14] S. Peng, H. Jiang, H. Wang, H. Alwageed and Y. Yao, ”Modulation classification using convolutional Neural Network based deep learning model,” 2017 26th Wireless and Optical Communication Conference (WOCC), Newark, NJ, 2017, pp. 1-5, doi: 10.1109/WOCC.2017.7929000.

[15] P. Kiran, M. G. Jibukumar and C. V. Premkumar, ”Resource allocation optimization in LTE-A/5G networks using big data analytics,” 2016 International Conference on Information Networking (ICOIN), Kota Kinabalu, 2016, pp. 254-259, doi: 10.1109/ICOIN.2016.7427072.

[16] D. He, C. Liu, T. Q. S. Quek and H. Wang, ”Transmit Antenna Selection in MIMO Wiretap Channels: A Machine Learning Approach,” in IEEE Wireless Communications Letters, vol. 7, no. 4, pp. 634-637, Aug. 2018, doi: 10.1109/LWC.2018.2805902.

[17] J. Xing, T. Lv and X. Zhang, ”Cooperative Relay Based on Machine Learning for Enhancing Physical Layer Security,” 2019 IEEE 30th Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC), Istanbul, Turkey, 2019, pp. 1-6, doi: 10.1109/PIMRC.2019.8904319.

[18] M. Kobayashi and M. Debbah, ”On the secrecy capacity of frequency-selective fading channels : A practical vandermonde precoding,” 2008 IEEE 19th International Symposium on Personal, Indoor and Mobile Radio Communications, Cannes, 2008, pp. 1-5, doi: 10.1109/PIMRC.2008.4699971.

[19] R. Negi and S. Goel, ”Secret communication using artificial noise,” VTC-2005-Fall. 2005 IEEE 62nd Vehicular Technology Conference, 2005., Dallas, TX, USA, 2005, pp. 1906-1910, doi: 10.1109/VETECF.2005.1558439.

[20] C. Wen, W. Shih and S. Jin, ”Deep Learning for Massive MIMO CSI Feedback,” in IEEE Wireless Communications Letters, vol. 7, no. 5, pp.748-751, Oct. 2018, doi: 10.1109/LWC.2018.2818160.

[21] P. Dong, H. Zhang and G. Y. Li, ”Machine Learning Prediction Based CSI Acquisition for FDD Massive MIMO Downlink,” 2018 IEEE Global Communications Conference (GLOBECOM), Abu Dhabi, United Arab Emirates, 2018, pp. 1-6, doi: 10.1109/GLOCOM.2018.8647328.

[22] Y. Sui, W. Yu and Q. Luo, ”Jointly Optimized Extreme Learning Machine for Short-Term Prediction of Fading Channel,” in IEEE Access, vol. 6, pp. 49029-49039, 2018, doi: 10.1109/ACCESS.2018.2868480.

[23] N. Nguyen, H. Q. Ngo, T. Q. Duong, H. D. Tuan and K. Tourki, ”Secure Massive MIMO With the Artificial Noise-Aided Downlink Training,” in IEEE Journal on Selected Areas in Communications, vol. 36, no. 4, pp.802-816, April 2018, doi: 10.1109/JSAC.2018.2825140.

[24] F. Zhu, F. Gao, H. Lin, S. Jin, J. Zhao and G. Qian, ”Robust Beamforming for Physical Layer Security in BDMA Massive MIMO,” in IEEE Journal on Selected Areas in Communications, vol. 36, no. 4, pp. 775-787, April 2018, doi: 10.1109/JSAC.2018.2824259.

[25] M. Mirzaee and S. Akhlaghi, ”Maximizing the minimum achievable secrecy rate in a two-user Gaussian interference channel,” 2014 Iran Workshop on Communication and Information Theory (IWCIT), Tehran, 2014, pp. 1-5, doi: 10.1109/IWCIT.2014.6842501.

[26] T. Liu and S. Shamai, ”A Note on the Secrecy Capacity of the Multiple-Antenna Wiretap Channel,” in IEEE Transactions on Information Theory, vol. 55, no. 6, pp. 2547-2553, June 2009, doi: 10.1109/TIT.2009.2018322.

[27] D. Wyner, ”The wire-tap channel”, Bell Syst. Tech. J., vol. 54, no. 8,pp.1355–1387, Oct. 1975.

[28] Z. Wang, D. W. K. Ng, V. W. S. Wong and R. Schober, ”Robust Beamforming Design in C-RAN With Sigmoidal Utility and Capacity-Limited Backhaul,” in IEEE Transactions on Wireless Communications, vol. 16, no. 9, pp. 5583-5598, Sept. 2017, doi: 10.1109/TWC.2017.2712645.

[29] B. Chen et al., ”Securing Uplink Transmission for Lightweight Single-Antenna UEs in the Presence of a Massive MIMO Eavesdropper,” in IEEE Access, vol. 4, pp. 5374-5384, 2016, doi: 10.1109/ACCESS.2016.2608932.

[30] W. C. Barott, ”Effect of beamforming errors on the efficacy of maximal ratio and equal gain combining,” IEEE SOUTHEASTCON 2014, Lexington, KY, 2014, pp. 1-4, doi: 10.1109/SECON.2014.6950738.

[31] I. F. Labaran, ”Spatial Modulation: A Comparison of maximum receiver ratio combining and maximum likelihood detectors,” 2014 11th International Conference on Electronics, Computer and Computation (ICECCO), Abuja, 2014, pp. 1-3, doi: 10.1109/ICECCO.2014.6997579.

[32] A. Haqiqatnejad, F. Kayhan and B. Ottersten, ”Robust Design of Power Minimizing Symbol-Level Precoder under Channel Uncertainty,” 2018 IEEE Global Communications Conference (GLOBECOM), Abu Dhabi, United Arab Emirates, 2018, pp. 1-6, doi: 10.1109/GLOCOM.2018.8647896.

[33] Z. B. Krusevac, P. B. Rapajic and R. A. Kennedy, ”On channel uncertainty modeling - an information theoretic approach,” IEEE Global Telecommunications Conference, 2004. GLOBECOM ’04., Dallas, TX, 2004, pp. 410-414 Vol.1, doi: 10.1109/GLOCOM.2004.1377980.

[34] S. Boyd and L. Vandenberghe, ”Convex Optimization” Cambridge University Press, 2004.

[35] E. Boshkovska, A. Koelpin, D. W. K. Ng, N. Zlatanov and R. Schober, ”Robust beamforming for SWIPT systems with non-linear energy harvesting model,” 2016 IEEE 17th International Workshop on Signal Processing Advances in Wireless Communications (SPAWC), Edinburgh, 2016, pp. 1-5, doi: 10.1109/SPAWC.2016.7536860.

[36] Z. Chu, K. Cumanan, Z. Ding, M. Johnston and S. Le Goff, ”Robust Outage Secrecy Rate Optimizations for a MIMO Secrecy Channel,” in IEEE Wireless Communications Letters, vol. 4, no. 1, pp. 86-89, Feb. 2015, doi: 10.1109/LWC.2014.2374611.

[37] M. Grant and S. Boyd, ”CVX: Matlab software for disciplined convex programming, version 2.2”, Mar. 2020. [Online]. Available: http://cvxr.com/cvx

[38] D. Stursa and P. Dolezel, ”Comparison of ReLU and linear saturated activation functions in neural network for universal approximation,” 2019 22nd International Conference on Process Control (PC19), Strbske Pleso, Slovakia, 2019, pp. 146-151, doi: 10.1109/PC.2019.8815057.

Appendices:

Appendix 1: Work plan and Gantt diagram

This section details how the work has been done during the evolution of the project. As detailed below, the initial steps of the project sought to find a research opportunity which was not covered by the state of the art before starting our study. After this analysis the direction of the project could be defined.

The project's work plan was divided in the following work packages:

Project: Considering research opportunities	**WP ref: WP0**	
Major constituent: Research and Documentation	Sheet 1	
Short description: **Reviews the current wireless communications state of the art. Provides a summary of topics that are currently being considered in ongoing research and proposes some research opportunities.**	Start date: 06/01/2020 End date: 17/01/2020 Start event: T1 End event: T4	
Internal task T1: Summary on big data based resource allocation **Internal task T2: Review of distributed data processing and machine learning** **Internal task T3: Summary of edge computing techniques** **Internal task T4: Research trends involving deep learning in wireless communications**	Deliverables: Research opportunities proposal	Dates: 17/01/2020

Table 3 Work package 0

Project: Review	**WP ref: WP1**	
Major constituent: Research and Documentation	Sheet 2	
Short description: **Research on the different topics needed during the project: physical layer security using machine learning, traditional techniques tackling physical layer security, physical layer security in massive MIMO, machine learning applied to CSI, etc.**	Start date: 17/01/2020 End date: 24/01/2020 Start event: T1 End event: T6	
Internal task T1: Definition of physical layer security	Deliverables:	Dates: 24/01/2020

Internal task T2: Machine learning applied to physical layer security: transmit antenna selection techniques, relays… **Internal task T3: Traditional techniques in physical layer security** **Internal task T4: Channel state information and deep learning** **Internal task T5: Massive MIMO framework** **Internal task T6: Artificial noise injection techniques**	Presentation of the findings	

Table 4 Work package 1

Project: System model definition	**WP ref: WP2**	
Major constituent: Theoretical approach	Sheet 3	
Short description: **System model definition: finding the problem to solve, modelling of the scenario and considerations about the designed wireless network.**	Start date: 24/01/2020 End date: 31/01/2020	
	Start event: T1 End event: T4	
Internal task T1: Finding the particular problem to solve **Internal task T2: Modelling of the network users: legitimate receivers, base station and eavesdroppers** **Internal task T3: Channel state information considerations** **Internal task T4: Physical resources used in the system**	Deliverables: System model proposal	Dates: 31/01/2020

Table 5 Work package 2

Project: Problem formulation	**WP ref: WP3**	
Major constituent: Formulation and coding	Sheet 4	
Short description: **Mathematical formulation to describe the problem and design of the convex optimization approach. Implementation in code of the mathematical formulation.**	Start date: 31/01/2020 End date: 06/03/2020	
	Start event: T1 End event: T4	
Internal task T1: Formulation of the received signals, SINRs, data rates and optimization problem proposals **Internal task T2: Cost function design and introducing uncertainty to the study**	Deliverables: Presenting the updates	Dates:

Internal task T3: Relaxing the non-convex problem **Internal task T4: Implementing the theoretical model**		07/02/2020 14/02/2020 21/02/2020 28/02/2020 06/03/2020

Table 6 Work package 3

Project: Learning system design	**WP ref: WP4**	
Major constituent: Review, analysis and coding	Sheet 5	
Short description: **Review state of the art deep learning techniques applied to wireless communications. Proposing a deep learning design to our approach. Design of the training set, neural networks required and architecture of the networks.**	Start date: 06/03/2020 End date: 27/03/2020	
	Start event: T1 End event: T5	
Internal task T1: Learning system objectives **Internal task T2: Classification neural networks** **Internal task T3: Architecture and reducing the sample data** **Internal task T4: Obtaining the training set** **Internal task T5: Training and testing the system**	Deliverables: Presenting the updates	Dates: 06/03/2020 13/03/2020 20/03/2020 27/03/2020

Table 7 Work package 4

Project: Simulations and adjustments	**WP ref: WP5**	
Major constituent: Coding	Sheet 6	
Short description: **Obtaining results achieved by the proposed tools.**	Start date: 27/03/2020 End date: 15/06/2020	
	Start event: T1 End event: T5	
Internal task T1: Generating beamforming codebooks and databases **Internal task T2: Hyperparameter tuning** **Internal task T3: Large training set trainings** **Internal task T4: Feature selection**	Deliverables: Presenting the updates	Dates:

Internal task T5: Performance results and modifications		27/03/2020 03/04/2020 10/04/2020 17/04/2020 24/04/2020 01/05/2020 08/05/2020 15/05/2020 22/05/2020 29/05/2020 05/06/2020 12/06/2020 19/06/2020

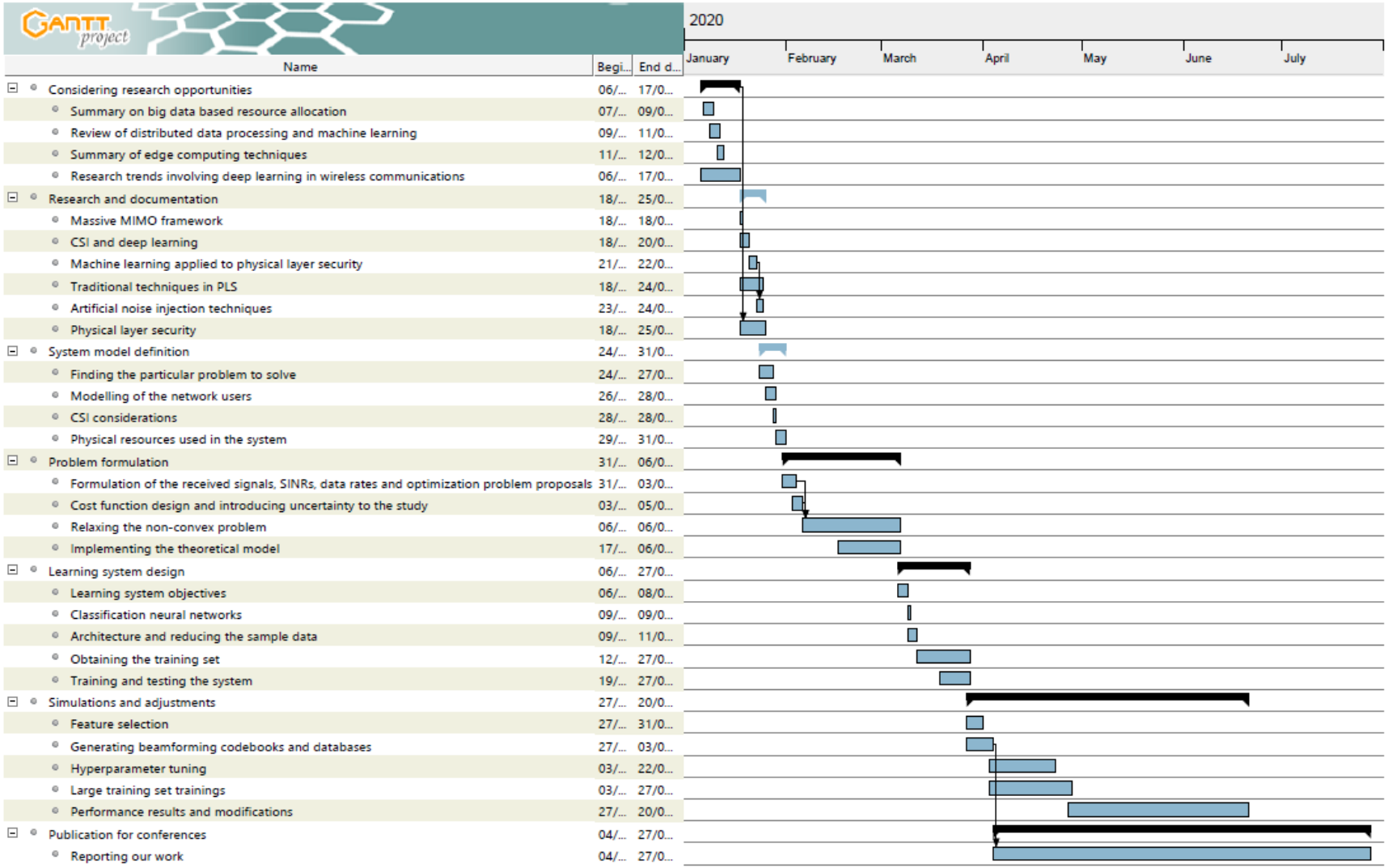
Table 8 Work package 5

Project: Publication for conferences	**WP ref: WP6**	
Major constituent: Reporting	Sheet 7	
Short description: **Reporting our study to prepare conference publications.**	Start date: 27/03/2020 End date: 05/06/2020	
	Start event: T1 End event: T1	
Internal task T1: Reporting our work	Deliverables: Presenting the updates	Dates:

		27/03/2020 03/04/2020 10/04/2020 17/04/2020 24/04/2020 01/05/2020 08/05/2020 15/05/2020 22/05/2020 29/05/2020 05/06/2020 12/06/2020 19/06/2020

Table 9 Work package 6

The Gantt diagram is the following:



Name	Begi...	End d...
Considering research opportunities	06/...	17/0...
Summary on big data based resource allocation	07/...	09/0...
Review of distributed data processing and machine learning	09/...	11/0...
Summary of edge computing techniques	11/...	12/0...
Research trends involving deep learning in wireless communications	06/...	17/0...
Research and documentation	18/...	25/0...
Massive MIMO framework	18/...	18/0...
CSI and deep learning	18/...	20/0...
Machine learning applied to physical layer security	21/...	22/0...
Traditional techniques in PLS	18/...	24/0...
Artificial noise injection techniques	23/...	24/0...
Physical layer security	18/...	25/0...
System model definition	24/...	31/0...
Finding the particular problem to solve	24/...	27/0...
Modelling of the network users	26/...	28/0...
CSI considerations	28/...	28/0...
Physical resources used in the system	29/...	31/0...
Problem formulation	31/...	06/0...
Formulation of the received signals, SINRs, data rates and optimization problem proposals	31/...	03/0...
Cost function design and introducing uncertainty to the study	03/...	05/0...
Relaxing the non-convex problem	06/...	06/0...
Implementing the theoretical model	17/...	06/0...
Learning system design	06/...	27/0...
Learning system objectives	06/...	08/0...
Classification neural networks	09/...	09/0...
Architecture and reducing the sample data	09/...	11/0...
Obtaining the training set	12/...	27/0...
Training and testing the system	19/...	27/0...
Simulations and adjustments	27/...	20/0...
Feature selection	27/...	31/0...
Generating beamforming codebooks and databases	27/...	03/0...
Hyperparameter tuning	03/...	22/0...
Large training set trainings	03/...	27/0...
Performance results and modifications	27/...	20/0...
Publication for conferences	04/...	27/0...
Reporting our work	04/...	27/0...

Glossary

2G: Second generation mobile network.

4G: Fourth generation mobile network.

5G: Fifth generation mobile network.

BS: Base station.

CSI: Channel state information.

eMBB: Enhanced mobile broadband.

I.i.d: Independent and identically distributed.

IoT: Internet of things.

KKT: Karush-Kuhn-Tucker.

KPI: Key performance indicator.

LMI: Linear Matrix Inequality.

MIMO: Multiple-input and multiple-output.

mMTC: Massive machine type communications.

MNO: Mobile network operator.

OFDM: Orthogonal frequency-division multiplexing.

OSI: Open system intercommunication.

RAN: Radio access network.

SINR: Signal-to-interference-plus-noise ratio.

SVD: Singular value decomposition.

TDD: Time division duplex.

UE: User equipment.

URLLC: Ultra-reliable low-latency communications.